MATH1061 — Week 1 Notes

Table of contents

Lecture 1 — Welcome & Warm-up Problems **2**
- Objectives for the hour . . . 2
- Warm-up problems . . . 3
- Solution 1 — parity of $p+r$, pr and $r-p$ . . . 3
- Solution 2 — showing $ac<0$ . . . 4
- Solutions 3, 4 and 5 . . . 5
- What each problem previews . . . 7
- See also . . . 8

Lecture 3 — Conditional Statements **9**
- Learning goals . . . 9
- Common questions . . . 9
- Conditional ($\rightarrow$) . . . 9
- Worked: equivalents and negation of a conditional . . . 11
- Worked: the inverse is not the negation . . . 12
- Order of operations (extended) . . . 12
- Worked: an equivalence proved two ways . . . 12
- Necessary and sufficient conditions . . . 13
- Worked: conditions for divisibility by 6 . . . 14
- See also . . . 15

Lecture 2 — Logical Form and Logical Equivalence **15**
- Learning goals . . . 15
- Common questions . . . 16
- Statements . . . 16
- Worked: translating between English and symbols . . . 16
- Truth tables . . . 17
- Inclusive and exclusive or . . . 17
- Order of operations . . . 18
- Worked: constructing a truth table . . . 18

Logical equivalence . . . 18
De Morgan's Laws . . . 20
The laws of logical equivalence . . . 20
Worked: one equivalence, by truth table and by the laws . . . 21
See also . . . 22

Reference material **22**
Conditional & Biconditional Statements . . . 22
Euler Circuits and Trails . . . 27
The Examination Formula Page . . . 38
Graphs . . . 42
Logical Connectives . . . 50
Logical Equivalence & Laws . . . 56
Diagram and Notation Conventions . . . 60
The Pigeonhole Principle . . . 77
Practice Problems — the Semester-wide Set . . . 85
Proof Techniques — Direct, Counterexample, Contradiction, Contraposition . . . 210
Solving Recurrence Relations . . . 219

Lecture 1 — Welcome & Warm-up Problems

Two halves: administration — staff, expectations, support, assessment, the topic list and the schedule — and five warm-up problems that preview the rest of the semester. Everything administrative is in math1061[1]. The few course rules that matter most are repeated here, followed by the problems.

Objectives for the hour

- Introduce the lecturing staff.
- Review course expectations, the course profile and the course website.
- Support mechanisms.
- Explain the assessment structure.
- Topics overview.

The load-bearing bits of the course rules:

- **Lectures are Mon 10am, Tue 2pm, Thu 1pm** — see the table in math1061[2].
- **General enquiries go to a course address, not a personal one**: `math1061@uq.edu.au` and `math7861@uq.edu.au`.

[1] courses/math1061/math1061.pdf
[2] courses/math1061/math1061.pdf

- **The pre-class hour is two things**: watch videos **and** answer multiple-choice questions. Both, not just the videos.
- Among the activities: the **Active Class**, and **Complete Assessed Exercises**.
- In the assessment: **best 8 of 12**, and the **hurdles** on the final exam.

Warm-up problems

1. Let p, q and r be consecutive positive integers with $p < q < r$, and let

$$a = p + r, \qquad b = pr, \qquad c = r - p.$$

   Determine which of a, b, c must be even.

2. Four non-zero real numbers a, b, c, d are given, where $b + d \neq 0$. If $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a+c}{b+d}$, show that $ac < 0$.

3. True or False: In every group of five people, there are two people who have the same number of friends within the group.

4. **The Tower of Hanoi**: Given a tower of 8 discs in decreasing size on one of three pegs, transfer the entire tower to one of the other pegs according to the following rules: (a) Move only one disc at a time. (b) Never move a larger disc onto a smaller disc. Is there a solution? If there is, what is the fewest number of moves needed to complete the transfer?

5. **The Königsberg Bridge Problem**: Does there exist a route through the city that crosses each bridge exactly once and takes you back to the starting place? (No turning around on bridges.)

The short answers to the last three: **3** — **True**, **4** — **255**, **5** — **No**. Problems 1 and 2 are worked in full below.

Solution 1 — parity of $p + r$, pr and $r - p$

Start with examples, not algebra: $1, 2, 3$, then $5, 6, 7$, then $2, 3, 4$. In each triple look at p **and** r, the first and last. What matters is their **parity** (even/odd): p and r are always two apart, so they are always the same kind of number.

Written out: p, q, r are consecutive, so

$$q = p + 1 \qquad \text{and} \qquad r = p + 2.$$

$a = p + r$ **is always even.** Since $r = p + 2$, the numbers p and r are both even or both odd, and even + even = even and odd + odd = even. Either way a is even.

$b = pr$ **is either even or odd**, and that is the whole answer. If p and r are even then pr is even; if both are odd then pr is odd. Nothing forces one case over the other, so b need not be even.

$c = r - p$ **is always even**, and more than that, it is always exactly 2:

$$c = r - p = (p + 2) - p = 2.$$

So a **and** c **must be even;** b **need not be.**

consecutive $\Rightarrow q = p + 1$ and $r = p + 2$, so p and r are two apart
$\Rightarrow p, r$ always share their parity, and $c = r - p = 2$ always

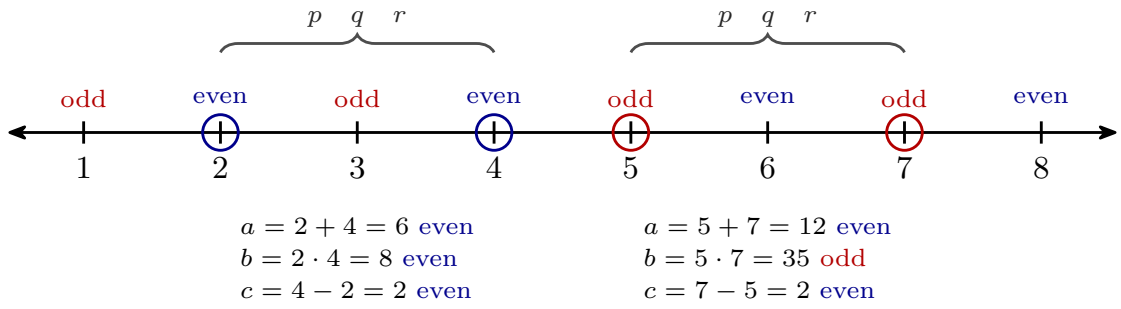


Figure 1: Why two of the three expressions are forced. Consecutive integers alternate parity, so p and r — two apart — always match, which makes p+r even and pinches r−p down to the constant 2; only the product pr is free to go either way. The two windows are the triples 2,3,4 and 5,6,7, with p and r ringed and a, b, c worked out beneath each. Blue marks even and red odd throughout.

Nothing in this solution is more than the definition of "consecutive" plus the two parity facts. That is the shape every direct proof in proof-techniques[3] takes from Lecture 7 onwards. For b, *"either even or odd"* is a complete answer to "which **must** be even", because a single pair of examples on opposite sides settles it.

Solution 2 — showing $ac < 0$

The proof is one algebraic chain, ending in an argument about signs:

Suppose $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a + c}{b + d}$.

[3] courses/math1061/proof-techniques.pdf

Put the left side over a common denominator:

$$\frac{ad}{bd} + \frac{bc}{bd} = \frac{a+c}{b+d}$$

Multiply both sides by $bd(b+d)$ — legitimate because $b, d \neq 0$ and $b+d \neq 0$, which is exactly why the question hands you those conditions. The bd cancels on the left and the $b+d$ on the right:

$$bd\,(b+d)\left(\frac{ad+bc}{bd}\right) = \left(\frac{a+c}{b+d}\right)(b+d)\,bd$$

$$(ad+bc)(b+d) = (a+c)\,bd$$

Expand the left side (**FOIL**):

$$abd + ad^2 + b^2c + bcd = abd + bcd$$

The abd and bcd terms cancel from both sides, leaving

$$ad^2 + b^2c = 0, \qquad \text{i.e.} \qquad ad^2 = -b^2c.$$

Divide both sides by ab^2 (allowed: $a \neq 0$ and $b \neq 0$):

$$\frac{d^2}{b^2} = -\frac{c}{a}$$

The left side is a square over a square with $d \neq 0$, so it is **positive**; therefore $-\frac{c}{a}$ is positive, so $\frac{c}{a}$ is **negative**. A negative quotient means **exactly one of a and c is negative**, so their product is negative. $\therefore\ ac < 0$.

Two habits here that the rest of the course keeps asking for. First, every non-zero hypothesis gets used at the moment it licenses a division — the three conditions $b \neq 0$, $d \neq 0$, $b+d \neq 0$ are not decoration. Second, the final step reasons about **sign**, not about values: $\frac{c}{a} < 0$ says one of the two is negative without saying which, and that is already enough for $ac < 0$.

The symbol $\therefore$ reads "Therefore". It prefixes the conclusion of an argument all semester (see math1061-diagram-notation[4]).

Solutions 3, 4 and 5

Each of these answers is the punchline of a topic later in the semester.

[4] courses/math1061/math1061-diagram-notation.pdf

3. True — and it is the pigeonhole principle

True. Each of the five people has a friend count somewhere in $\{0, 1, 2, 3, 4\}$ — five people, five possible values, so counting alone is not enough. The extra fact is that 0 **and** 4 **cannot both occur**: if someone is friends with all four others, then nobody has zero friends; and if someone has zero friends, nobody can be friends with all four. So the counts actually available are only four values, and five people distributed over four values must repeat one. That is the pigeonhole principle, which arrives in **Lecture 33** — see pigeonhole-principle[5], where the same argument is made for the degrees of a graph, and practice-problems[6].

(This assumes friendship is mutual, which is what "friends within the group" is taken to mean.)

4. 255 moves

255. The reasoning comes in Lecture 16 and is worked in full at solving-recurrence-relations[7]: letting m_n be the minimum number of moves for n discs, moving the largest disc forces the other $n-1$ onto the spare peg and back again, giving

$$m_1 = 1, \qquad m_k = 2m_{k-1} + 1 \ \text{ for } k \geq 2,$$

whose explicit formula is $m_n = 2^n - 1$. For eight discs, $2^8 - 1 = 255$. The answer to "is there a solution?" is yes, and constructively so — the recursion *is* the algorithm.

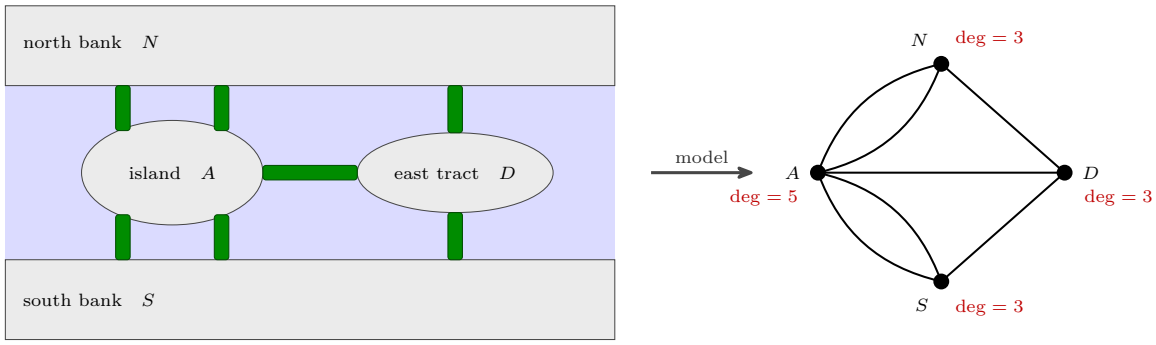
5. No

No. The modelling step is to redraw the map of Königsberg, a river crossed by seven bridges, as a graph. Graph theory is introduced at Lecture 33; the graph theory lectures are L33–L36. Graphs, loops, multiple edges and degree are defined in [graphs].

The question as asked is for a **closed** route — one that returns to where it started. Such a route must leave every land mass exactly as often as it enters it, so every bridge at a land mass is used in an entry/exit pair, and **every vertex must have even degree**. Here all four are odd, so no closed route exists.

Keep the two criteria apart. The standard slogan is about the *open* case: an open route crossing every bridge once (not required to return) exists only when the number of odd-degree vertices is 0 or 2. Königsberg has four, so that fails too — but "more than two odd vertices" is not the criterion for the question as asked.

[5] courses/math1061/pigeonhole-principle.pdf
[6] courses/math1061/practice-problems.pdf
[7] courses/math1061/solving-recurrence-relations.pdf



schematic of the city

the seven bridges, in green

every degree odd ⇒ no closed route

Figure 2: The modelling step. Each land mass becomes a vertex and each bridge an edge, so the seven bridges become seven edges on four vertices — and the question 'can I walk every bridge once and get back?' becomes a question about degrees. Every vertex here has odd degree, and a closed route must enter and leave each land mass in pairs, so no such route exists. The left panel is a schematic of the city, with the land masses named A, N, S and D and the bridges in green; the right panel is the same city as a graph.

Both criteria are the two halves of one theorem about connected graphs: an **Euler circuit** exists exactly when every vertex has even degree, and an **Euler trail** between two different vertices exactly when those two are the only odd ones. The theorem, its proof and how to find such a route are in euler-circuits-and-trails[8], and Lecture 34 (2026-10-26-walks-trails-and-circuits[9]) applies it.

What each problem previews

Problem	Previews	Lecture
1 — parity of $p+r$, pr, $r-p$	direct proof, definitions of even/odd, number theory	L7 (proof-techniques[10])
2 — showing $ac < 0$	direct proof from an algebraic hypothesis; using every hypothesis	L7 (proof-techniques[11])

[8] courses/math1061/euler-circuits-and-trails.pdf
[9] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[10] courses/math1061/proof-techniques.pdf
[11] courses/math1061/proof-techniques.pdf

Problem	Previews	Lecture
3 — five people, same friend count	the pigeonhole principle	L33 (pigeonhole-principle[12])
4 — Tower of Hanoi	recursion, recurrence relations, induction	L13–L16 (solving-recurrence-relations[13])
5 — Königsberg bridges	graph theory, walks and circuits	L33–L34 ([graphs], euler-circuits-and-trails[14])

That table is the course outline in miniature — logic and proof first, then number theory, sets, functions and relations, group theory, counting, and graph theory last. Fields and probability belong to the same stretch of the semester; see math1061[15] for the course profile's topic list. Some of this **overlaps Year 11 and 12 Specialist Mathematics**.

See also

- math1061[16] — staff, assessment weights, support, and the lecture schedule
- math1061-diagram-notation[17] — the course's own notation and figure conventions
- 2026-07-30-logical-form-and-equivalence[18] — Lecture 2, where the symbolic logic starts properly
- proof-techniques[19] — the four proof methods problems 1 and 2 are a warm-up for
- solving-recurrence-relations[20] — the Tower of Hanoi recurrence worked in full
- euler-circuits-and-trails[21] — the theorem that settles the bridges of Königsberg
- practice-problems[22] — the semester-wide practice problem set, with solutions; it belongs to the individual-study hours, not the class (the logic sections begin at practice-problems[23])

[12] courses/math1061/pigeonhole-principle.pdf
[13] courses/math1061/solving-recurrence-relations.pdf
[14] courses/math1061/euler-circuits-and-trails.pdf
[15] courses/math1061/math1061.pdf
[16] courses/math1061/math1061.pdf
[17] courses/math1061/math1061-diagram-notation.pdf
[18] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[19] courses/math1061/proof-techniques.pdf
[20] courses/math1061/solving-recurrence-relations.pdf
[21] courses/math1061/euler-circuits-and-trails.pdf
[22] courses/math1061/practice-problems.pdf
[23] courses/math1061/practice-problems.pdf

Lecture 3 — Conditional Statements

Pre-work: Video 003 (Conditional Statements). See conditional-statements[24] for the reference definitions this lecture builds on. **Note**: Applied Classes start in Week 2, and they include an assessed component.

The proofs of $\sim((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \equiv p$ — one by truth table and two by chains of laws — are at the end of Lecture 2[25].

Learning goals

1. Understand the connectives *if…then* ($\rightarrow$) and *if and only if* ($\leftrightarrow$).
2. Be familiar with common logical equivalences involving *if…then*:

$$p \rightarrow q \equiv \sim p \vee q \equiv \sim q \rightarrow \sim p$$

   Know this — the two rewrites are the whole toolkit for everything below.
3. Be able to negate a conditional statement.
4. Understand the meaning of necessary and sufficient conditions.

Common questions

- **How can $p \rightarrow q$ be true when p is false?** Because that is how it is defined. The bottom two rows of the table are a definition, not a claim about the world.
- **Can we use any laws for "p implies q"?** Replace $p \rightarrow q$ with $\sim p \vee q$ and then use the laws. The laws of logical equivalence are stated only for $\sim, \wedge, \vee$, so this substitution is what gives you access to them.
- **For necessary and sufficient conditions, which one signifies IF, and which ONLY IF?** "If" is the *sufficient* half, "only if" is the *necessary* half.

Conditional ($\rightarrow$)

p	q	$p \rightarrow q$
T	T	T
T	F	**F**
F	T	T
F	F	T

[24] courses/math1061/conditional-statements.pdf
[25] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf

Exactly one row makes it false: **true hypothesis, false conclusion**. See the containment figure in conditional-statements[26]: the situations making p true sit **inside** the situations making q true, which is why nothing outside p can falsify the conditional.

By definition — this is also called the **disjunctive form** of $\rightarrow$ —

$$p \rightarrow q \ \equiv \sim p \vee q$$

Contrapositive, converse, inverse

Name	Form	
Conditional	$p \rightarrow q$	**logically equivalent** to each other
Contrapositive	$\sim q \ \rightarrow \sim p$	
Converse	$q \rightarrow p$	**logically equivalent** to each other
Inverse	$\sim p \ \rightarrow \sim q$	

Reminder: $p \rightarrow q \not\equiv q \rightarrow p$. The four forms and the only equivalences among them are laid out as a figure in conditional-statements[27].

English phrasings

$p \rightarrow q$ can be expressed in many ways in English. The following are logically equivalent:

- p implies q
- If p then q
- q **if** p
- p is **sufficient** for q
- p **only if** q
- q is **necessary** for p

Watch where the letters land: "q if p" puts the hypothesis *second*, and "p only if q" puts the hypothesis *first*. Those two lines are the ones worth memorising, because they are the ones the necessary/sufficient vocabulary is built on.

Biconditional

$$p \leftrightarrow q \ \equiv \ (p \rightarrow q) \wedge (q \rightarrow p)$$

[26] courses/math1061/conditional-statements.pdf
[27] courses/math1061/conditional-statements.pdf

Worked: equivalents and negation of a conditional

(a) Which of the following statements have the same meaning as: "If the file is missing, then the program crashes"? (Multiple answers allowed.)

Let p = "the file is missing" and q = "the program crashes", so the statement is $p \to q$.

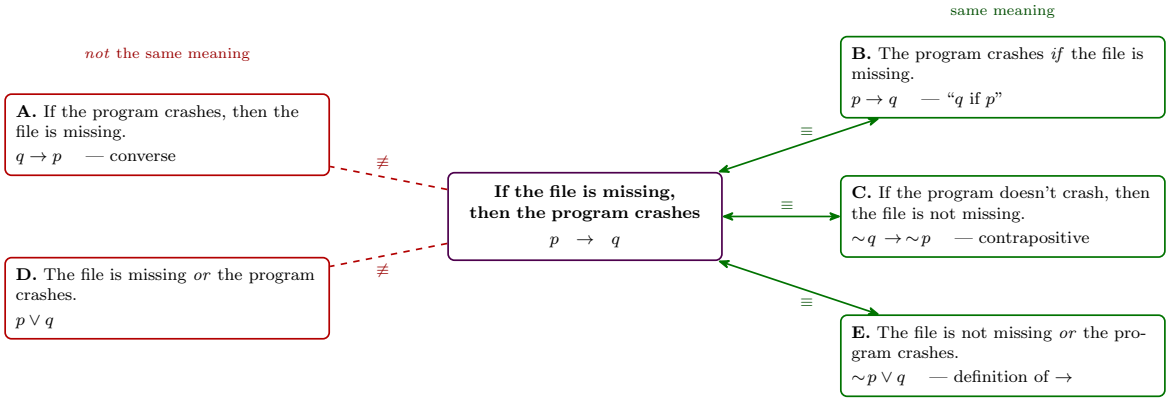


Figure 3: The five options and their verdicts, each translated into symbols: green has the same meaning as the original, red does not. The verdict follows from the symbols alone: B is the same conditional with the 'if' clause second, C is its contrapositive, E is its disjunctive form. A is the converse and D is a plain disjunction — neither is equivalent. Translate before judging: A and B are built from the same two clauses in the same order — all that moves is which clause the 'if' attaches to, and that alone reverses the conditional.

Answer: B, C and E.

(b) Write the NEGATION of the original statement.

$$\sim (p \to q) \;\equiv \sim (\sim p \vee q) \;\equiv\; p \wedge \sim q$$

by the definition of $\to$, then De Morgan's law and the double negative law. In English:

> **The file is missing but the program didn't crash.**

The negation of a conditional is an **and**, never another conditional.

Worked: the inverse is not the negation

Demonstrate that $\sim (p \to q) \not\equiv \sim p \to \sim q$.

> Let p be true and q be true. Then $(p \to q)$ is true, so $\sim (p \to q)$ is **false**. BUT $\sim p \to \sim q$ is **true**. $\therefore \sim (p \to q) \not\equiv \sim p \to \sim q$.

The third line holds because $\sim p \to \sim q$ evaluates as F $\to$ F, true by the bottom row of the table. This is the shape for demonstrating $\not\equiv$: name one assignment, evaluate both sides on it, then state the conclusion. No truth table required.

$\sim p \to \sim q$ is the **inverse** — offering it as the negation of $p \to q$ is the classic error that learning goal 3 is aimed at.

Order of operations (extended)

1. $\sim$
2. $\wedge, \vee$ (equal) — use parentheses to specify; if none, work from left to right
3. $\to, \leftrightarrow$ (equal) — use parentheses to specify; if none, work from left to right

So the statement form $p \to \sim q \vee r$ means $p \to ((\sim q) \vee r)$, **but parentheses should always be used to avoid confusion.**

Note on notation. The biconditional $\leftrightarrow$ is a connective, used to **combine** statements (similar to $+, -, \times, \div$ … with numbers). Logical equivalence $\equiv$ is used when **comparing** two statements (similar to $=$ with numbers). Do not blur the two: $a \leftrightarrow b$ is itself a statement, $a \equiv b$ is a claim about two statements.

Worked: an equivalence proved two ways

Let p, q and r be statements. Show that $p \to (q \vee r) \equiv (p \wedge \sim q) \to r$.

There are two solutions.

Solution 1 — one chain, all the way across:

$$\begin{aligned}
p \to (q \vee r) &\equiv \sim p \vee (q \vee r) && \text{by definition of } \to \\
&\equiv (\sim p \vee q) \vee r && \text{by the associative law} \\
&\equiv (\sim p \vee \sim\sim q) \vee r && \text{by the double negative law} \\
&\equiv \sim (p \wedge \sim q) \vee r && \text{by De Morgan's law} \\
&\equiv (p \wedge \sim q) \to r && \text{by definition of } \to
\end{aligned}$$

Solution 2 — work both sides down to the same thing:

$$
\begin{aligned}
\text{LHS:}\quad p \to (q \vee r) &\equiv \sim p \vee (q \vee r) && \text{definition of } \to \\
&\equiv (\sim p \vee q) \vee r && \text{associative} \\
\text{RHS:}\quad (p \wedge \sim q) \to r &\equiv \sim (p \wedge \sim q) \vee r && \text{definition of } \to \\
&\equiv (\sim p \vee q) \vee r && \text{De Morgan's and double negative}
\end{aligned}
$$

Both sides reach $(\sim p \vee q) \vee r$ — **the same** — so the two forms are equivalent.

Solution 2 avoids having to guess which direction to push a negation — each side is simplified independently until they meet. Both are complete proofs.

Necessary and sufficient conditions

> p is a **necessary condition** for q means "if $\sim p$ then $\sim q$", or equivalently "if q then p" $(q \to p)$, or "q **only if** p".
>
> p is a **sufficient condition** for q means "if p then q", or equivalently "q **if** p".

The two phrasings of *necessary* are contrapositives of each other, which is why they agree.

Worked — necessary but not sufficient. *Being a non-negative integer is necessary for a number to be the square of an integer, but it is not sufficient.*

- If a number is the square of an integer, then it is non-negative — so -9 **cannot** be the square of an integer.
- But 7 is a non-negative integer and is **not** the square of an integer, so the condition does not suffice.

Worked — sufficient but not necessary. *Being an integer that is divisible by 4 is sufficient for being an even integer, but it is not necessary.*

- 8 is divisible by 4, so we know that 8 is even — no further checking needed.
- But 10 is an even integer and is **not** divisible by 4, so the condition is not required.

Biconditional as necessary *and* sufficient

The three rows below say the same thing, and each splits at the same seam:

Whole statement		the **necessary** half		the **sufficient** half
$a \leftrightarrow b$	$\equiv$	$(a \to b)$	$\wedge$	$(b \to a)$
a if and only if b	$\equiv$	a **only if** b	and	a **if** b

Whole statement		the **necessary** half		the **sufficient** half
b is necessary and sufficient for a	$\equiv$	b is necessary for a	and	b is sufficient for a

Read down the third column and you get three names for one half of the biconditional; down the fifth, three names for the other. That answers the earlier question: **"only if" marks the necessary half, "if" marks the sufficient half.** The same table is a colour-aligned figure in conditional-statements[28].

Worked: conditions for divisibility by 6

Let n be a positive integer.

	Asked	Answer	Why
(a)	A condition **necessary but not sufficient** for n to be divisible by 6	n **is divisible by 3**	Every multiple of 6 is a multiple of 3, so it is necessary; $n = 3$ is divisible by 3 but not by 6, so it is not sufficient
(b)	A condition **sufficient but not necessary** for n to be divisible by 6	$n = 12$	12 is divisible by 6, so it suffices; $n = 6$ is divisible by 6 without being 12, so it is not necessary
(c)	A **necessary and sufficient** condition for n to be divisible by 6	n **is divisible by both 2 and 3**	Both directions hold, so this is a genuine biconditional

A *sufficient but not necessary* condition can be cheap — pinning n to a single value is sufficient for anything true of that value.

[28] courses/math1061/conditional-statements.pdf

See also

- conditional-statements[29] — the reference definitions, the four forms, and the necessary/sufficient vocabulary
- logical-equivalence-laws[30] — the laws used in the negation and the two-way proof above
- 2026-07-30-logical-form-and-equivalence[31] — Lecture 2 · 2026-08-03-valid-and-invalid-arguments[32] — Lecture 4
- practice-problems[33] — §3 Conditional Statements, with full worked solutions

Lecture 2 — Logical Form and Logical Equivalence

Pre-work: Video 001 (Logical Form), Video 002 (Logical Equivalence). See logical-connectives[34] and logical-equivalence-laws[35] for the reference definitions/tables this lecture builds on.

Logic is the study of reasoning. What the language of symbolic logic is *for* is worth keeping in view, because the rest of the logic block is in service of it. Symbolic logic will help us to:

- analyse ordinary sentences,
- test arguments for validity,
- construct proofs for complex arguments,
- identify incorrect proofs and common fallacies.

Learning goals

1. Appreciate the difficulties in translating between English and mathematics.
2. Understand the logical connectives $\sim$ (not), $\wedge$ (and), $\vee$ (or).
3. Construct a truth table for a statement form in standard form.
4. Use a truth table to establish logical equivalence of two statement forms.
5. Apply logical equivalence laws to establish logical equivalence of two statement forms.

[29] courses/math1061/conditional-statements.pdf
[30] courses/math1061/logical-equivalence-laws.pdf
[31] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[32] courses/math1061/2026-08-03-valid-and-invalid-arguments.pdf
[33] courses/math1061/practice-problems.pdf
[34] courses/math1061/logical-connectives.pdf
[35] courses/math1061/logical-equivalence-laws.pdf

Common questions

- **Can we use other symbols for "not"?** Yes — common symbols for *not* include $\sim$ and $\neg$. This course writes $\sim$.
- **How do we work out the number of variables and the number of rows in a truth table — for $(p \wedge q) \wedge (q \wedge r)$, are there 2 variables, 3 or 4? Each unique letter is a variable**, so here there are 3 variables p, q, r, and the truth table has $2^3 = 8$ rows. The repeated q does not count twice.
- **Do we need to memorise the laws of logical equivalence? No.** The laws are given on the examination formula page (see formula-sheet[36]).

Statements

A **statement** (or **proposition**) is a sentence that is either true or false, but not both.

- Statements: **"6 is odd."** — a statement, and **false**. **"It is raining."** — also a statement; it could be either true or false, and not knowing the value doesn't stop it having one.
- Not statements: **"x is odd."** (depends on the unspecified x), **"Is it raining?"** (a question), **"She is happy."** (not objectively true or false).

We use variables $p, q, r, \ldots$ to represent statements, and the connectives **and** $\wedge$, **or** $\vee$, **not** $\sim$ to combine them. See logical-connectives[37].

Worked: translating between English and symbols

Let p = "it is cold", q = "it is snowing", r = "it is sunny".

Into symbolic form:

English	Symbolic	Note
It is not cold **but** it is snowing.	$\sim p \wedge q$	"but" is $\wedge$ — the contrast it carries in English is invisible to logic
It is **neither** snowing **nor** cold, but it is sunny.	$\sim (q \vee p) \wedge r \equiv (\sim q \wedge \sim p) \wedge r$	"neither … nor" is **the negation of an "or" statement**; the second form is the De Morgan rewrite of the first

[36] courses/math1061/formula-sheet.pdf
[37] courses/math1061/logical-connectives.pdf

Into English:

Symbolic	English
$\sim q \wedge p$	It is not snowing and it is cold.
$(p \wedge q) \vee r$	It is cold and snowing, **or** it is sunny.

The $\vee$ in the second one is the **inclusive or** — a day that is cold, snowing *and* sunny satisfies it.

Are these equivalent statements? (1) "It is not cold but it is snowing." (2) "It is snowing and it is not cold."

Yes — by the commutative law. Symbolically $\sim p \wedge q \equiv q \wedge \sim p$. The English word order carries an emphasis the logic does not.

Truth tables

A truth table shows the truth value of a statement form for **all possible** truth values of its statement variables. With n variables it has 2^n rows. You should know the truth tables for $\wedge$, $\vee$ and $\sim$ by heart.

Build them in **standard form**, so that you are sure you have covered all combinations and it is easy for someone to check your work — the fixed row order is drawn out as a figure in logical-connectives[38].

Inclusive and exclusive or

$\vee$ means **inclusive or**: $p \vee q$ is true when p is true, or q is true, or both.

Sometimes English "or" means "one or the other but not both" — **exclusive or**, written $\oplus$ (XOR):

$$p \oplus q \;\equiv\; (p \vee q) \wedge (\sim (p \wedge q))$$

Setting $p \oplus q$ between $p \wedge q$ and $p \vee q$ makes the two differences visible:

p	q	$p \wedge q$	$p \oplus q$	$p \vee q$
T	T	T	F	T
T	F	F	T	T

[38] courses/math1061/logical-connectives.pdf

p	q	$p \wedge q$	$p \oplus q$	$p \vee q$
F	T	F	T	T
F	F	F	F	F

$$p \oplus q \not\equiv p \vee q \qquad\qquad p \oplus q \not\equiv p \wedge q$$

Examples from common English usage: *"Would you like red or white wine?"* is **exclusive** and *"Would you like milk or sugar with your tea?"* is **inclusive**. Only context distinguishes them — which is precisely learning goal 1.

Order of operations

1. $\sim$ first.
2. $\wedge$ and $\vee$ equal second — use parentheses to specify; if no parentheses, work from left to right.

Worked. Take the statement form $(p \wedge q) \vee \sim (r \vee p) \wedge s$. This means

$$\big((p \wedge q) \vee (\sim (r \vee p))\big) \wedge s$$

$\sim$ takes only $(r \vee p)$; the remaining $\vee$ and $\wedge$ are then equal in precedence, so they resolve left to right.

Worked: constructing a truth table

Construct a truth table for $(p \wedge \sim q) \vee (q \wedge r)$.

There are two ways to lay this out: give each sub-expression its **own column** ($\sim q$, then $p \wedge \sim q$, then $q \wedge r$, then the whole thing), or work **all at once**, writing each column of values directly beneath the part of the expression it evaluates. The figure below uses the column-by-column layout, because a single column can then be checked in isolation.

Logical equivalence

Given two statement forms, you can show that they **are logically equivalent** ($\equiv$) using a truth table or the laws of logical equivalence. To show that two statement forms are **not logically equivalent** ($\not\equiv$), you need to find a set of truth values for the variables for which the two statement forms have **opposite** truth values.

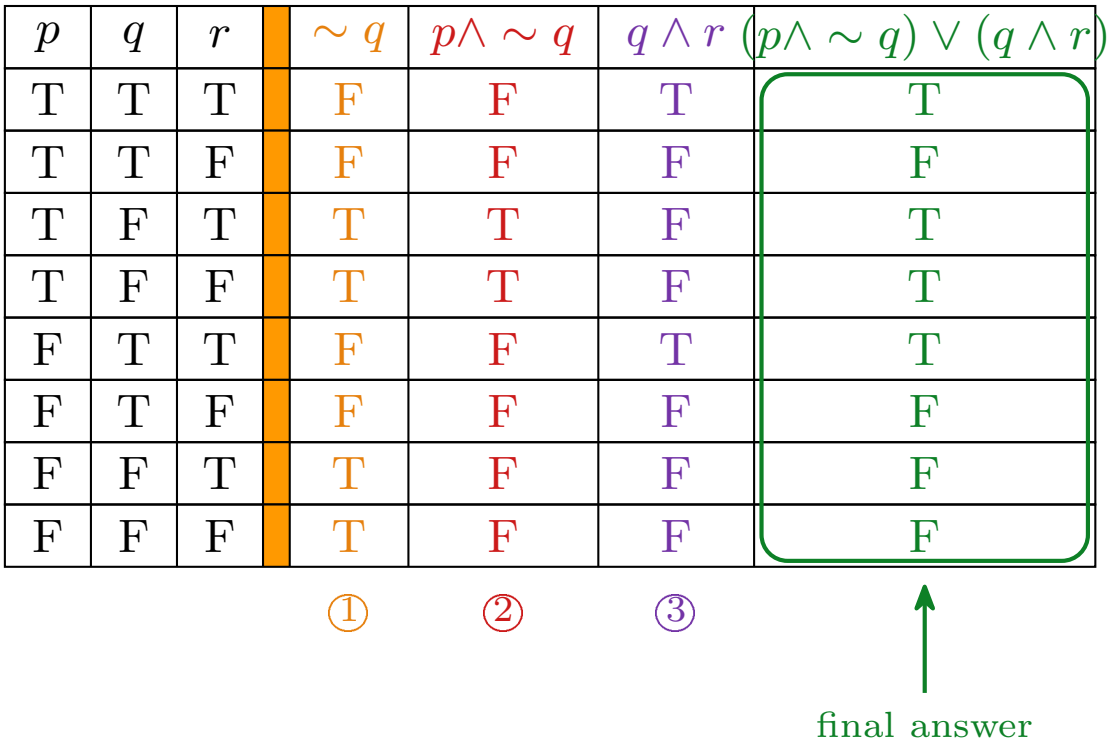


Figure 4: The truth table for (p ~q) (q r), laid out column by column. The evaluation order is numbered beneath — ~q first, then p ~q, then q r — and the outlined last column is the final answer. Laid out this way, any one column can be checked in isolation.

Worked: a non-equivalence from one row

Show that $\sim (p \vee q) \not\equiv \sim p \vee \sim q$**.**

Take p **false** and q **true**:

- LHS: $p \vee q$ is $\mathrm{F} \vee \mathrm{T} = \mathrm{T}$, so $\sim (p \vee q)$ is **false**.
- RHS: $\sim p \vee \sim q$ is $\mathrm{T} \vee \mathrm{F} = \mathrm{T}$, so it is **true**.

They differ on this assignment, so they are **not logically equivalent**. One row is a complete answer — there is no need to fill in the other three.

De Morgan's Laws

Important logical equivalences for the negations of statements involving "and" and "or":

$$\sim (p \wedge q) \equiv \sim p \vee \sim q \qquad\qquad \sim (p \vee q) \equiv \sim p \wedge \sim q$$

Both halves get negated **and** the connective flips. The non-equivalence above is what happens when you flip the sign but forget the connective.

Worked: negating an "and" statement

Write down a statement which is logically equivalent to the NEGATION of: "5 is divisible by 2 and 6 is divisible by 2."

> **5 is not divisible by 2 or 6 is not divisible by 2.**

(The original is $p \wedge q$ with $p =$ "5 is divisible by 2" and $q =$ "6 is divisible by 2", so its negation is $\sim p \vee \sim q$. As it happens the negation is true and the original false, but that is not what was asked — the question is about *form*.)

The laws of logical equivalence

The full table is in logical-equivalence-laws[39]; it is the one on the examination formula page. Two definitions used throughout it:

- a **tautology t** is a statement that is **always true**;
- a **contradiction c** is a statement that is **always false**.

[39] courses/math1061/logical-equivalence-laws.pdf

Worked: two proofs with the laws

Show that $(p \wedge \sim q) \wedge (\sim p \vee q) \equiv \mathbf{c}$.

$$
\begin{aligned}
(p \wedge \sim q) \wedge (\sim p \vee q) &\equiv (p \wedge \sim q) \wedge \ \sim (p \wedge \sim q) && \text{by De Morgan's law and the double negative law} \\
&\equiv r \wedge \sim r \quad \text{where } r = (p \wedge \sim q) \\
&\equiv \mathbf{c} && \text{by the negation law}
\end{aligned}
$$

The move that makes it short is recognising $\sim p \vee q$ as $\sim (p \wedge \sim q)$ — a whole compound expression standing in for the single letter the law is written with.

Show that $\sim p \vee (p \wedge q) \ \equiv \sim p \vee q$.

$$
\begin{aligned}
\sim p \vee (p \wedge q) &\equiv (\sim p \vee p) \wedge (\sim p \vee q) && \text{by the distributive law} \\
&\equiv \mathbf{t} \wedge (\sim p \vee q) && \text{by the negation law} \\
&\equiv \sim p \vee q && \text{by the identity law}
\end{aligned}
$$

Worked: one equivalence, by truth table and by the laws

(a) Use a truth table to show that $\sim ((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \equiv p$.

p	q	$\sim p$	$\sim q$	$\sim p \wedge q$	$\sim p \wedge \sim q$	$(\sim p \wedge q) \vee (\sim p \wedge \sim q)$	$\sim (\cdots)$
T	T	F	F	F	F	F	**T**
T	F	F	T	F	F	F	**T**
F	T	T	F	T	F	T	**F**
F	F	T	T	F	T	T	**F**

The first column and the last column are **identical**, so $\sim ((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \equiv p$. Marking the two columns that have to match — with a $*$ beneath each — and then stating the verdict in words is how to finish a truth-table equivalence proof. The table alone does not say what it has shown.

(b) Use the laws of logical equivalence to show the same.

There are two complete chains, one six steps and one four. Both are drawn side by side as a figure in logical-equivalence-laws[40]; the short one comes from noticing that $\sim p$ is a common factor of the two disjuncts and pulling it out with the distributive law before doing anything else.

[40] courses/math1061/logical-equivalence-laws.pdf

See also

- logical-connectives[41] · logical-equivalence-laws[42] — the reference definitions and the full table of equivalence laws
- formula-sheet[43] — why the laws don't need memorising
- 2026-07-30-conditional-statements[44] — Lecture 3
- practice-problems[45] — §1 Logical Form, with full worked solutions
- practice-problems[46] — §2 Logical Equivalence, with full worked solutions

Reference material

Conditional & Biconditional Statements

Conditional ($\rightarrow$)

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Only one row makes a conditional false: the row where the hypothesis p is true and the conclusion q is false. Everything else is true, including both rows where p is false.

$p \rightarrow q$ is true when p is false **because that is how it is defined.** There is no deeper intuition to recover; $\rightarrow$ is a truth-functional connective fixed by the table above, and arguing with the bottom two rows is arguing with a definition. The standard name for those two rows is **vacuous truth**. It does real work later: it is why $\emptyset \subseteq A$ for every set A (see sets-and-set-notation[47]).

The picture behind the table is containment:

[41] courses/math1061/logical-connectives.pdf
[42] courses/math1061/logical-equivalence-laws.pdf
[43] courses/math1061/formula-sheet.pdf
[44] courses/math1061/2026-07-30-conditional-statements.pdf
[45] courses/math1061/practice-problems.pdf
[46] courses/math1061/practice-problems.pdf
[47] courses/math1061/sets-and-set-notation.pdf

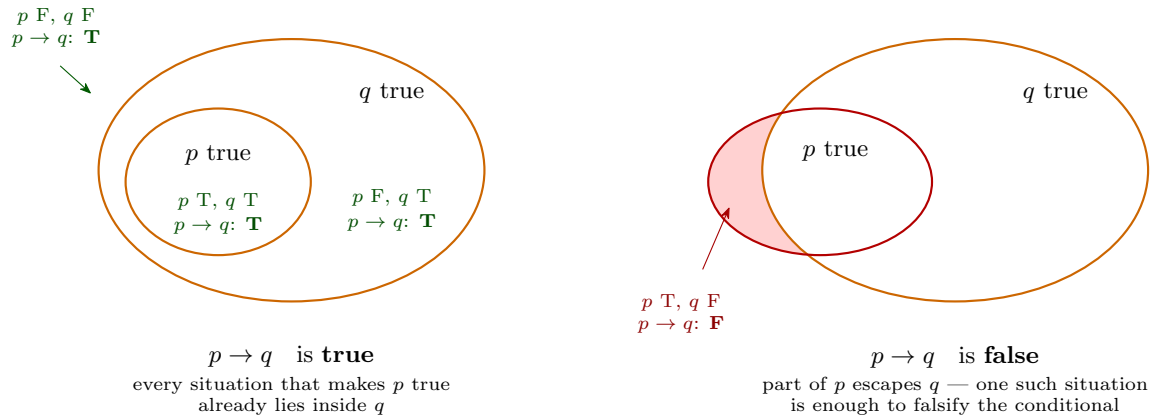


Figure 5: Why the truth table has the shape it does. Left: p → q asserts that the situations making p true all lie inside the situations making q true, so every region carries T. Right: the conditional fails exactly when part of p escapes q, which is the single F row of the table.

Disjunctive form

By definition,

$$p \to q \ \equiv \sim p \vee q$$

The right-hand side is the **disjunctive form** of the conditional, and it is the single most useful fact in the topic: the laws of logical equivalence (see logical-equivalence-laws[48]) are stated only for $\sim$, $\wedge$ and $\vee$, so they say nothing about $\to$ directly. To use the laws on a conditional:

> **Replace $p \to q$ with $\sim p \vee q$ and then use the laws.**

Every worked proof about conditionals in this course starts and (usually) ends with that substitution.

$p \to q$ can be phrased: "p implies q", "if p then q", "q if p", "p is sufficient for q", "p only if q", "q is necessary for p".

Warning: $p \to q \not\equiv q \to p$.

Contrapositive, converse, inverse

[48] courses/math1061/logical-equivalence-laws.pdf

Name	Form	Equivalent to
Conditional	$p \to q$	Contrapositive
Contrapositive	$\sim q \to \sim p$	Conditional
Converse	$q \to p$	Inverse
Inverse	$\sim p \to \sim q$	Converse

The conditional and its **contrapositive** are always logically equivalent. The **converse** and **inverse** are always logically equivalent to each other — but *not* to the original conditional.

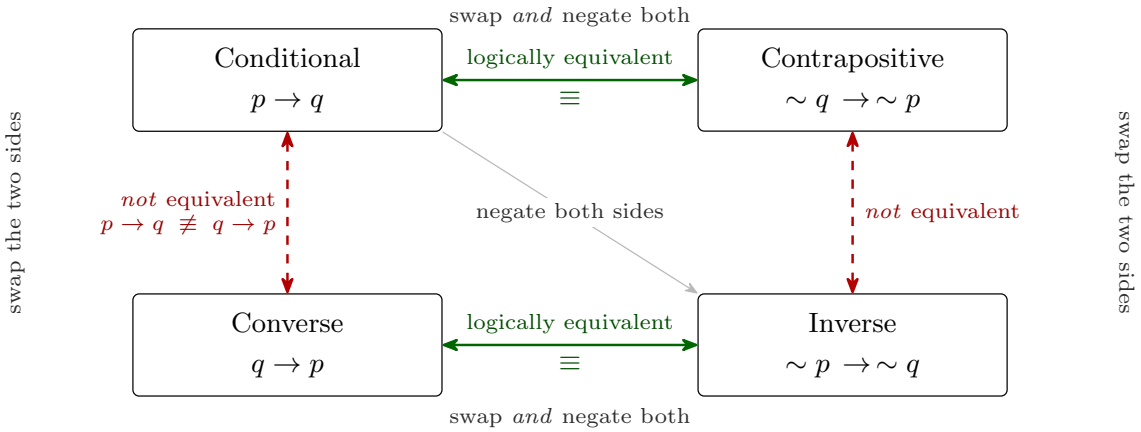


Figure 6: The four forms and the only equivalences among them. The conditional and the contrapositive are one logically equivalent pair, the converse and the inverse are the other, and p → q q → p. Swapping the two sides gives the converse, negating both gives the inverse, and doing both gives the contrapositive — the only one of the three that preserves meaning.

Both equivalences fall straight out of the disjunctive form. For the first: $p \to q \equiv \sim p \vee q$ and $\sim q \to \sim p \equiv \sim(\sim q) \vee \sim p \equiv q \vee \sim p$, which is the same disjunction commuted. The converse/inverse pair is the same computation with p and q interchanged.

Necessary and sufficient conditions

- p is a **necessary condition** for q means "if $\sim p$ then $\sim q$", or equivalently "if q then p", or "q **only if** p". In symbols, $q \to p$.
- p is a **sufficient condition** for q means "if p then q", or equivalently "q **if** p". In symbols, $p \to q$.

The two phrasings of "necessary" are contrapositives of each other, which is why they say the same thing: $\sim p \rightarrow \sim q$ and $q \rightarrow p$.

The reliable reading is: **"if" introduces the sufficient condition; "only if" introduces the necessary one.**

Worked: necessary but not sufficient

Being a non-negative integer is necessary for a number to be the square of an integer, but it is not sufficient.

- *Necessary*: if a number is the square of an integer, then it is non-negative. So -9 cannot be the square of an integer — failing the condition rules the number out.
- *Not sufficient*: 7 is a non-negative integer but it is not the square of an integer. Meeting the condition does not settle it.

Worked: sufficient but not necessary

Being an integer that is divisible by 4 is sufficient for being an even integer, but it is not necessary.

- *Sufficient*: if an integer is divisible by 4, then it is even. 8 is divisible by 4, so we know 8 is even without checking anything else.
- *Not necessary*: 10 is an even integer but 10 is not divisible by 4. The condition can fail while the conclusion still holds.

The two shapes are exactly opposite in how they are refuted: a claimed **sufficient** condition is killed by something satisfying the condition but not the conclusion; a claimed **necessary** condition is killed by something satisfying the conclusion but not the condition.

Biconditional ($\leftrightarrow$)

$$a \leftrightarrow b \equiv (a \rightarrow b) \wedge (b \rightarrow a)$$

A biconditional is the two one-way conditionals conjoined, and each of the standard English phrasings splits along the same seam:

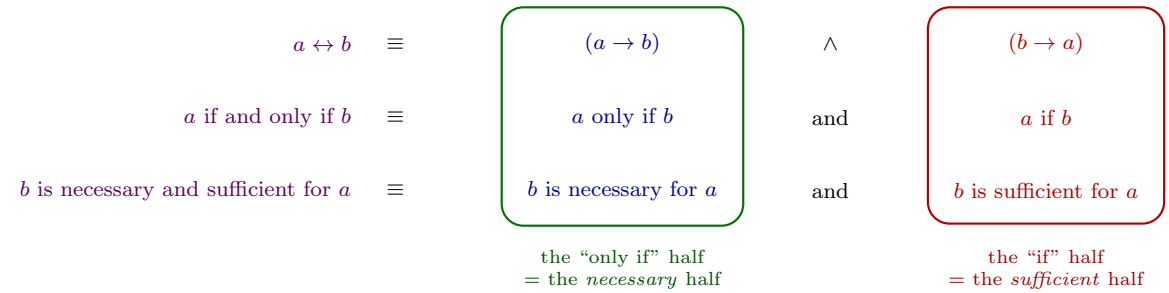


Figure 7: The biconditional decomposed three ways, with each half in its own ringed column. Reading down the left column: a → b, 'a only if b', 'b is necessary for a' are three names for the same half. Reading down the right: b → a, 'a if b', 'b is sufficient for a'. The whole necessary/sufficient vocabulary is just this correspondence — 'only if' is the necessary half, 'if' is the sufficient half.

Negating a conditional

$$\sim (p \to q) \equiv \sim (\sim p \vee q) \equiv p \wedge \sim q$$

by the definition of →, then De Morgan's law, then the double negative law.

The negation of a conditional is not a conditional — it's an *and*. "If it rains, the match is cancelled" is negated by "it rains **and** the match is not cancelled", not by "if it rains, the match is not cancelled".

The classic error is to answer $\sim p \to \sim q$ (that's the *inverse*) or $q \to p$ (the *converse*). Neither is the negation, and neither is even equivalent to the original — see Figure 6 above.

Worked: $\sim (p \to q) \not\equiv \sim p \to \sim q$**.** Let p be **true** and q be **true**. Then $p \to q$ is true, so $\sim (p \to q)$ is **false**. But $\sim p \to \sim q$ is F → F, which is **true**. The two differ on this row, so they are not equivalent.

Sanity check on the shapes: $\sim (p \to q)$ is a conjunction and is true on exactly **one** of the four rows; $\sim p \to \sim q$ is a conditional and is true on **three**. They could hardly be equivalent.

Order of operations

1. ∼
2. ∧, ∨ (equal)
3. →, ↔ (equal)

Within a tier, work left to right if no parentheses are given. So $p \to \sim q \vee r$ means $p \to ((\sim q) \vee r)$ — but parenthesise explicitly rather than relying on the tie-breaking rule.

Notation, not to be blurred: the biconditional $\leftrightarrow$ is a connective used to **combine** statements (like $+$, $-$, $\times$, $\div$ with numbers). Logical equivalence $\equiv$ is used when **comparing** two statements (like $=$ with numbers). $a \leftrightarrow b$ is a statement; $a \equiv b$ is a claim *about* two statements.

See also

- logical-connectives[49]
- logical-equivalence-laws[50]
- sets-and-set-notation[51] — vacuous truth doing real work, in $\emptyset \subseteq A$
- 2026-07-30-conditional-statements[52] — Lecture 3
- practice-problems[53] — §3 Conditional Statements, with full worked solutions

Euler Circuits and Trails

An Euler circuit goes along every edge of a graph exactly once and comes back to where it started. An Euler trail does the same but finishes somewhere else. Whether a graph has one is decided by two things only: whether it is connected once its isolated vertices are set aside, and how many of its vertices have odd degree. None gives an Euler circuit, exactly two gives an Euler trail from one of them to the other, and any other number gives neither. This note has the definitions, the theorem with a full proof, how to actually find a circuit or trail, a flowchart for deciding, and how this course's definition differs from the textbook's. It builds on walks, trails, circuits and connectedness in walks-trails-and-circuits[54], and on degree in graphs[55]. First met in 2026-10-26-walks-trails-and-circuits[56].

Euler circuits

> An **Euler circuit** is a circuit that contains every edge of the graph.

[49] courses/math1061/logical-connectives.pdf
[50] courses/math1061/logical-equivalence-laws.pdf
[51] courses/math1061/sets-and-set-notation.pdf
[52] courses/math1061/2026-07-30-conditional-statements.pdf
[53] courses/math1061/practice-problems.pdf
[54] courses/math1061/walks-trails-and-circuits.pdf
[55] courses/math1061/graphs.pdf
[56] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf

A circuit never uses an edge twice (walks-trails-and-circuits[57]), so an Euler circuit uses **every edge exactly once** and ends where it started. It may pass through a vertex many times. A graph that has an Euler circuit is called **Eulerian**.

A graph with no edges has an Euler circuit: the trivial circuit at any vertex contains every edge, since there are none.

Euler trails

> An **Euler trail from vertex u to vertex v** is a trail that starts at u and ends at v and contains every edge of the graph.

The difference from an Euler circuit is only where it finishes. Both use every edge exactly once. An Euler circuit ends at the vertex it started from. An Euler trail from u to v ends at v, and the case that matters is $u \neq v$, an open route. (An Euler circuit is a trail from a vertex to itself, but the theorem below is about $u \neq v$.)

For a connected graph the two cannot both happen with $u \neq v$: the theorem says an Euler circuit needs every degree even, and an Euler trail from u to $v \neq u$ needs u and v odd.

The theorem

> **Theorem.** Let G be a connected graph. Then G has an Euler circuit if and only if every vertex of G has even degree.
>
> Let $u, v \in V(G)$ be distinct vertices of G. Then G has an Euler trail from u to v if and only if u and v have odd degree and all other vertices of G have even degree.

Every graph has an even number of vertices of odd degree (graphs[58]), so for a connected graph there are three cases: no odd vertices gives an Euler circuit, exactly two gives an Euler trail between them, and four or more gives neither.

Counting edge ends along a trail

Both directions of the proof rest on one count. Take a trail $T = v_0\, e_1\, v_1 \cdots e_n\, v_n$ and a vertex w. The edge e_i has its two ends at v_{i-1} and v_i (both at the same vertex if it is a loop). So the number of edge ends at w that T uses is

$$\underbrace{\#\{\, i : v_{i-1} = w \,\}}_{\text{times } T \text{ leaves } w} + \underbrace{\#\{\, i : v_i = w \,\}}_{\text{times } T \text{ arrives at } w}.$$

[57] courses/math1061/walks-trails-and-circuits.pdf
[58] courses/math1061/graphs.pdf

These ends are all different, because the edges of a trail are all different. Reading along the sequence, each arrival at w is followed by a departure, except an arrival at the very end, and each departure is preceded by an arrival, except a departure at the very start. So:

- **If w is not the first or last vertex**, T arrives at w exactly as often as it leaves: every pass through w uses **two** ends, one in and one out, and the number used is even.
- **If T is a circuit** ($v_0 = v_n$), the departure at the start and the arrival at the end pair up at v_0, and every vertex has an even number of ends used.
- **If** $v_0 \neq v_n$, T leaves v_0 once more than it arrives, and arrives at v_n once more than it leaves. At those two vertices the number of ends used is **odd**.

A loop at w is an arrival at w and a departure from w at once, and uses two ends at w, so it never changes these parities.

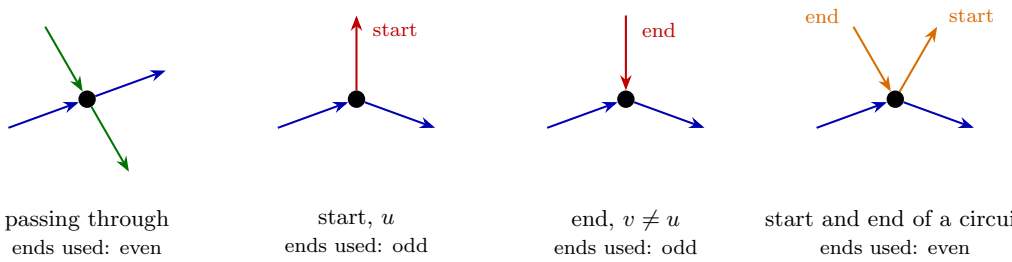


Figure 8: Edge ends used by a trail at one vertex. Arrows show the direction of travel. Left: a vertex in the middle of the trail. Each time the trail passes through, it arrives along one edge and leaves along another, so the ends pair up, blue with blue and green with green, and an even number is used. Second: the start of a trail that ends elsewhere has one departure with no arrival to pair with, in red, so an odd number is used. Third: the end of such a trail has one arrival left over. Right: at the start of a circuit, the first departure pairs with the final arrival, so every end pairs up again.

Proof: every edge used forces the degrees

Proof that an Euler circuit or trail forces the degrees. Suppose T is an Euler circuit of G. It uses every edge exactly once, so it uses every edge end in G exactly once, and the number of ends it uses at a vertex w is all of them, $\deg(w)$. By the count above that number is even. So every vertex has even degree.

Suppose instead T is an Euler trail from u to v with $u \neq v$. Again the ends used at w number $\deg(w)$. By the count, that is odd for $w = u$ and $w = v$, and even for every other vertex. □

This direction does not use connectedness.

Proof: even degrees give an Euler circuit

The construction rests on one fact about walking until stuck.

Lemma (stuck only at the start). Let H be a graph in which every vertex has even degree, and w a vertex with $\deg(w) \geq 1$. Start at w and build a trail one edge at a time: from the current vertex, go along any edge at it that has not been used yet, and stop when there is none. Then this stops, and it stops at w, so it produces a non-trivial circuit through w.

Proof. Each step uses a new edge and there are finitely many, so it stops. Suppose it is at a vertex $x \neq w$, having arrived there. The trail so far starts at w and ends at $x \neq w$, so by the count it has used an odd number of the ends at x. Since $\deg(x)$ is even, some end at x is unused, and the edge it belongs to is unused, because an edge is used all at once. So the trail can go on, and it does not stop at x. It therefore stops at w. It started along an edge, since $\deg(w) \geq 1$, so the circuit has at least one edge. □

Removing a circuit keeps every degree even. If C is a circuit and its edges are deleted (keeping all the vertices), each vertex loses the ends of it that C used, an even number by the count. Even minus even is even.

Proof of the theorem, circuits. Let G be connected with every vertex of even degree. Every vertex is a trivial circuit, so G has circuits. A circuit uses each edge at most once, so it has at most $|E(G)|$ edges, and there is a circuit $C = v_0\, e_1\, v_1 \cdots e_n\, v_n$ with **as many edges as possible**. Suppose, for a contradiction, that some edge of G is not in C.

Let H be G with the edges of C deleted. H has every vertex of even degree and at least one edge.

Some vertex of C has an edge in H. Take an edge of H and an endpoint x of it. If x is on C, done. If not, G is connected, so there is a walk in G from x to v_0. The walk starts off C and ends on C, so there is a first vertex y on it that lies on C, and the vertex z just before y is not on C. The edge f of the walk joining z and y is not an edge of C, since every edge of C has both endpoints on C. So f is in H, and its endpoint y is on C. Call this vertex w.

Splice. w has degree at least 1 in H, so the lemma, applied in H, gives a non-trivial circuit $C' = w\, f_1\, u_1 \cdots f_m\, w$ using only edges of H. w is on C, say $w = v_k$. Replace that one occurrence of v_k in C by the whole of C':

$$v_0\, e_1\, v_1 \cdots e_k\, \underbrace{v_k\, f_1\, u_1 \cdots f_m\, v_k}_{C'}\, e_{k+1} \cdots e_n\, v_n.$$

This is a walk, since C' leaves from v_k and returns to v_k. Its edges are those of C and those of C', which are all different, since the edges of C' are in H and H has none of the edges of C. So it is a trail, and it starts and ends at $v_0 = v_n$, so it is a circuit. It has $n + m > n$ edges, contradicting the choice of C.

So C contains every edge of G, and it is an Euler circuit. □

If G has no edges, C is a trivial circuit and nothing is missing. Connectedness is used in exactly one place: to get from an unused edge back to the circuit.

Proof: two odd vertices give an Euler trail

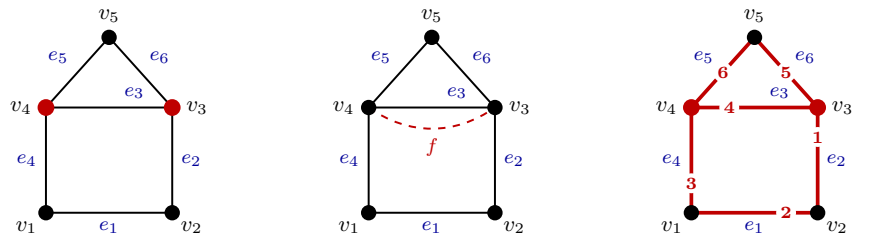
Proof of the theorem, trails. Let G be connected, with $u \neq v$ of odd degree and every other vertex of even degree. Make a new graph G' by adding one new edge f with endpoints u and v. If u and v are already adjacent, f is a parallel edge, and that is fine. In G', u and v each gain one end, so every vertex of G' has even degree, and G' is still connected. By the circuit case, G' has an Euler circuit C.

C uses f once, either as $\cdots u\, f\, v \cdots$ or as $\cdots v\, f\, u \cdots$. Read backwards if necessary (walks-trails-and-circuits[59]) so that it is $\cdots v\, f\, u \cdots$. Then start the circuit at that u, so that f is the last edge:

$$C = u \cdots v\, f\, u.$$

Delete the final $f\, u$. What is left is a trail, since its edges are some of the distinct edges of C. It starts at u, ends at v, uses every edge of G' except f exactly once, and so uses every edge of G exactly once. It is an Euler trail from u to v. □

Together with the first direction, that proves the theorem.



G: $\deg v_3 = \deg v_4 = 3$ G': add f, all degrees even Euler trail from v_3 to v_4

Figure 9: The trail case from the circuit case. Left: the house graph, connected, with v_3 and v_4 of odd degree, in red, and the others even. Middle: adding a new edge f joining v_3 and v_4, dashed, makes every degree even, so there is an Euler circuit, for example $v_3, e_2, v_2, e_1, v_1, e_4, v_4, e_3, v_3, e_6, v_5, e_5, v_4, f, v_3$, which ends with f. Here f is a second edge between two vertices that were already adjacent. Right: drop the final f. What is left, $v_3, e_2, v_2, e_1, v_1, e_4, v_4, e_3, v_3, e_6, v_5, e_5, v_4$, is an Euler trail from v_3 to v_4, in red with its edges numbered in order.

[59] courses/math1061/walks-trails-and-circuits.pdf

This course's definition and the textbook's

This course uses the standard definitions above: an Euler circuit contains every **edge**. The textbook defines an Euler circuit as a circuit that contains **every vertex and every edge** of the graph, and an Euler trail likewise.

They differ only when there are vertices that no edge touches. A triangle together with one isolated vertex has an Euler circuit by this course's definition (go once round the triangle), and none by the textbook's, because no circuit can reach the isolated vertex.

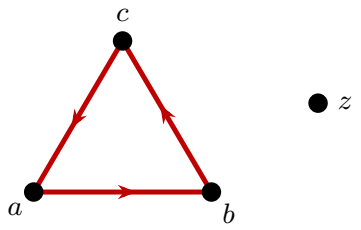


Figure 10: A triangle and an isolated vertex z. Going once round the triangle, in red, uses every edge, so by this course's definition it is an Euler circuit. By the textbook's definition it is not, since it misses z, and no circuit can visit z. The graph is disconnected, so the theorem does not apply to it as it stands. Deleting z leaves a connected graph with all degrees even.

For a connected graph the two definitions agree. A circuit or trail that contains every vertex and every edge certainly contains every edge. Conversely, let G be connected and let T contain every edge.

- If G has at least one edge, then every vertex is the endpoint of some edge. With a single vertex, every edge is a loop at it. With two or more vertices, take any vertex x and another vertex y: there is a walk from x to y, and its first edge has x as an endpoint. T uses that edge, so T passes through x.
- If G has no edges, being connected means it has one vertex. The only walk in G is that single vertex, so T is the trivial circuit there, and it contains the vertex.

So T contains every vertex too. The theorem assumes G is connected, so it says the same thing under either definition. The definitions only part ways for disconnected graphs whose edges all lie in one piece, with isolated vertices as the rest, such as the triangle and isolated vertex, and that case is what the first two steps of the flowchart deal with.

How to find one

The theorem says whether an Euler circuit or trail exists. To write one down, I use the splicing method that the proof is built on (it is usually called Hierholzer's algorithm):

1. **Check first.** Delete isolated vertices, check the rest is connected, and count the vertices of odd degree. None: look for a circuit, starting anywhere. Two, u and v: look for a trail, **starting at** u.
2. **Walk until stuck.** From the start, keep going along edges not used yet, choosing freely, until there are none at the current vertex. For a circuit this always stops back at the start (the lemma). For a trail from u it always stops at v: by the count, at any other vertex the trail has used an odd number of ends of an even-degree vertex, or, at u, an even number of ends of an odd-degree vertex, and either way an end is left.
3. **If edges are left, splice.** The unused edges give every vertex even degree, since what was walked used an even number of ends at each vertex except u and v, and an odd number at those two. Pick a vertex already on the route that still has an unused edge. Walk from it along unused edges until stuck. That is back at the same vertex. Insert this circuit into the route at that vertex.
4. **Repeat** step 3 until every edge is used.

When walking, it helps to tick off each edge on the drawing as it is used, and to write the route as a list of vertices (with edge names where there are multiple edges).

Another method avoids splicing by choosing carefully as you go (Fleury's algorithm): walk from the start, and at each step **don't burn your bridges**, that is, never use an edge whose removal would cut the unused edges into two separate pieces, unless it is the only edge left at the vertex. It gives the circuit or trail in one pass, but checking every step for a bridge is slow by hand, so I splice.

Worked: an Euler circuit by splicing

> Find an Euler circuit of the graph below: six vertices, each joined to every other vertex except one, the vertex "opposite" it. The non-adjacent pairs are v_1, v_6; v_2, v_4; v_3, v_5.

There are 12 edges, $v_1v_2, v_1v_3, v_1v_4, v_1v_5, v_2v_3, v_2v_5, v_2v_6, v_3v_4, v_3v_6, v_4v_5, v_4v_6, v_5v_6$. The graph is connected and every vertex has degree 4, so there is an Euler circuit. The graph is simple, so a route can be written as a list of vertices.

Walk until stuck. From v_1:

$$v_1\, v_2\, v_3\, v_1\, v_4\, v_5\, v_1.$$

At v_1 all four edges are now used, so this is stuck, back at the start, with 6 edges. Left over: $v_2v_5, v_2v_6, v_3v_4, v_3v_6, v_4v_6, v_5v_6$.

First splice. v_2 is on the route and still has the unused edges v_2v_5 and v_2v_6. Walk from v_2 along unused edges: $v_2\, v_5\, v_6\, v_2$, stuck at v_2. Insert it where the route passes v_2:

$$v_1\ \underbrace{v_2\, v_5\, v_6\, v_2}_{\text{inserted}}\ v_3\, v_1\, v_4\, v_5\, v_1.$$

Left over: v_3v_4, v_3v_6, v_4v_6.

Second splice. v_3 is on the route and still has unused edges. Walk from it: $v_3\, v_4\, v_6\, v_3$. Insert it where the route passes v_3:

$$v_1\, v_2\, v_5\, v_6\, v_2\ \underbrace{v_3\, v_4\, v_6\, v_3}_{\text{inserted}}\ v_1\, v_4\, v_5\, v_1.$$

That uses all 12 edges, each once, and returns to v_1: an Euler circuit.

Deciding: the flowchart

For any graph, connected or not:

Why each step is right:

- **No edges.** The trivial circuit at any vertex contains every edge, so there is an Euler circuit. This uses this course's definition: by the textbook's, a graph with two or more vertices and no edges would have none.
- **Deleting isolated vertices** changes no edge, so it does not change which routes use every edge. A route that uses every edge never needs to visit an isolated vertex.
- **Not connected, after deleting isolated vertices.** Then there are vertices x and y with no walk between them, and each has an edge, since nothing isolated is left. A circuit or trail containing both edges would contain a walk from x to y. So there is neither.
- **Connected.** Now the theorem applies. The number of odd-degree vertices is even (graphs[60]), so 0, 2, or 4 or more covers everything.

[60] courses/math1061/graphs.pdf

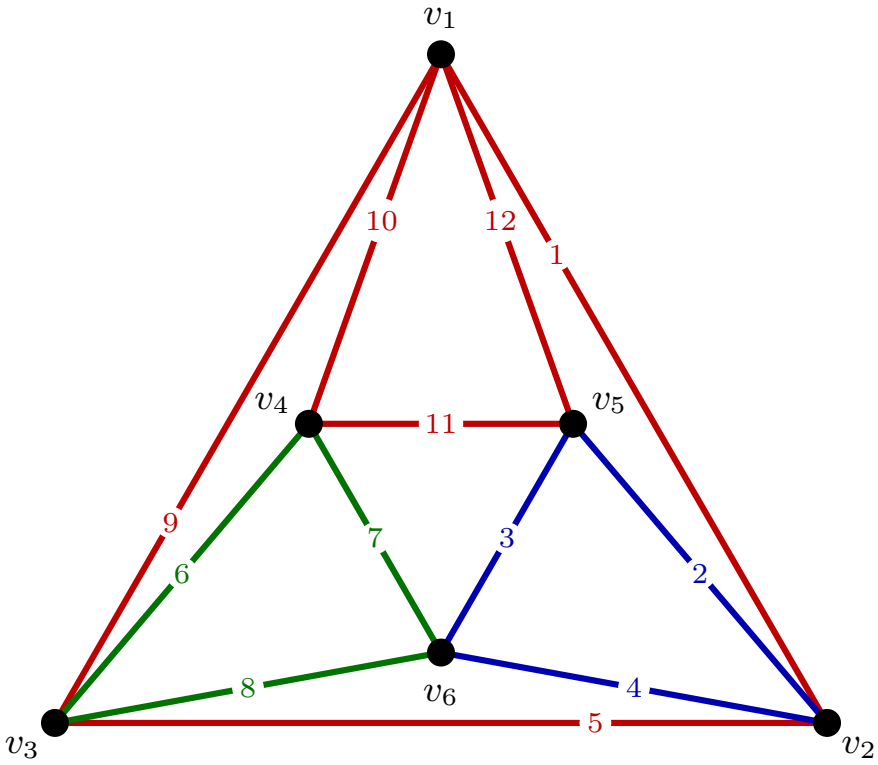


Figure 11: Finding an Euler circuit by splicing. Red: the first circuit, $v_1, v_2, v_3, v_1, v_4, v_5, v_1$, walked from v_1 until stuck. Blue: the circuit v_2, v_5, v_6, v_2 through v_2, built from unused edges and spliced in at v_2. Green: the circuit v_3, v_4, v_6, v_3 through v_3, spliced in at v_3. The small numbers give the order of the edges in the final circuit, $v_1, v_2, v_5, v_6, v_2, v_3, v_4, v_6, v_3, v_1, v_4, v_5, v_1$.

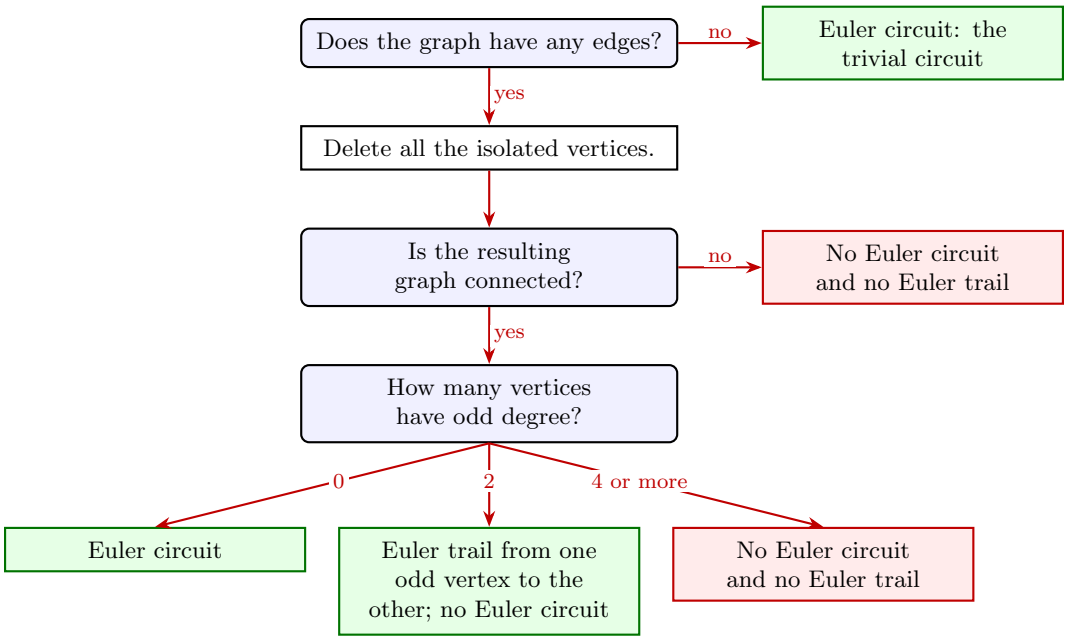


Figure 12: Deciding whether a graph has an Euler circuit or an Euler trail. A graph with no edges has one, the trivial circuit. Otherwise isolated vertices are deleted, since no edge touches them, and what is left must be connected, or some two edges cannot be on one route. Then the number of vertices of odd degree decides, and it is always even: none gives an Euler circuit, exactly two gives an Euler trail from one to the other, and four or more gives neither.

The bridges of Königsberg

The problem that started graph theory: the city of Königsberg had four land masses joined by seven bridges, and the question was whether there is a walk around the city crossing every bridge exactly once, ideally returning to the start. As a graph, the land masses are the vertices and the bridges the edges. The island has degree 5 and each of the other three land masses has degree 3 (2026-10-26-walks-trails-and-circuits[61] has the graph).

All four vertices have odd degree. The graph is connected, so by the theorem there is **no Euler circuit**, since that needs every degree even, and **no Euler trail** either, since that needs exactly two odd vertices. No walk crosses every bridge exactly once, whether or not it returns. The problem is set up in 2026-07-27-welcome-and-intro-problems[62].

Common mistakes

- **Forgetting connectedness.** Even degrees are not enough. Two separate circuits, such as two triangles, have every degree even and no Euler circuit. Check that the graph is connected, after deleting isolated vertices, before using the degrees.
- **Letting isolated vertices decide.** An isolated vertex makes the graph disconnected but does not stop an Euler circuit, by this course's definition. Delete them first. (By the textbook's definition they do stop one, which is why the definitions are compared above.)
- **Counting a loop as 1.** A loop adds 2 to the degree (graphs[63]), so loops never change whether a degree is odd or even.
- **Exactly two odd vertices gives a trail, not a circuit.** The trail must start at one odd vertex and end at the other. Starting at an even vertex will not work.
- **Zero odd vertices gives a circuit, and the trail part of the theorem does not apply.** An Euler circuit is also a trail from a vertex to itself, but the trail statement in the theorem is about $u \neq v$. With every degree even there is no Euler trail from u to a **different** v, since that would need u and v odd.
- **Getting stuck and concluding there is none.** Walking until stuck can leave edges unused even when an Euler circuit exists. That is not a failure: splice in the rest (how to find one). Only the degrees and connectedness decide existence.

See also

- walks-trails-and-circuits[64] — walks, trails, circuits and connected graphs
- [graphs] — degree, loops and the Handshake Theorem

[61] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[62] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[63] courses/math1061/graphs.pdf
[64] courses/math1061/walks-trails-and-circuits.pdf

- 2026-10-26-walks-trails-and-circuits[65] — Lecture 34, with worked questions on the theorem and an Euler trail on ten vertices
- 2026-07-27-welcome-and-intro-problems[66] — the bridges of Königsberg
- trees[67] — connected graphs with no non-trivial circuits
- practice-problems[68] — §44, with full worked solutions

The Examination Formula Page

The *MATH1061/MATH7861 Examination Formula Page* is **provided in both exams**, which are otherwise closed book with no written materials permitted (see math1061[69]). Knowing what is on it — and what is not — is what decides whether a fact needs memorising.

It has **seven blocks**.

1. Logical equivalences

Eleven named laws, given any statement variables p, q, r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$. Reproduced in full in logical-equivalence-laws[70].

Commutative · Associative · Distributive · Identity · Negation · Double negative · Idempotent · Universal bound · De Morgan's · Absorption · Negations of $\mathbf{t}$ and $\mathbf{c}$.

2. Valid argument forms

Nine forms. Reproduced in full in valid-argument-forms[71].

Modus Ponens · Modus Tollens · Generalization (a)(b) · Specialization (a)(b) · Conjunction · Elimination (a)(b) · Transitivity · Proof by division into cases · Contradiction Rule.

3. Set identities

Twelve numbered laws, for all sets A, B, C that are subsets of a universal set U:

[65] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[66] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[67] courses/math1061/trees.pdf
[68] courses/math1061/practice-problems.pdf
[69] courses/math1061/math1061.pdf
[70] courses/math1061/logical-equivalence-laws.pdf
[71] courses/math1061/valid-argument-forms.pdf

	Law	
1	Commutative	$A \cup B = B \cup A$ · $A \cap B = B \cap A$
2	Associative	$(A \cup B) \cup C = A \cup (B \cup C)$ · $(A \cap B) \cap C = A \cap (B \cap C)$
3	Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ · $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4	Identity	$A \cup \emptyset = A$ · $A \cap U = A$
5	Complement	$A \cup A^c = U$ · $A \cap A^c = \emptyset$
6	Double complement	$(A^c)^c = A$
7	Idempotent	$A \cup A = A$ · $A \cap A = A$
8	Universal bound	$A \cup U = U$ · $A \cap \emptyset = \emptyset$
9	De Morgan's	$(A \cup B)^c = A^c \cap B^c$ · $(A \cap B)^c = A^c \cup B^c$
10	Absorption	$A \cup (A \cap B) = A$ · $A \cap (A \cup B) = A$
11	Complement of U and $\emptyset$	$U^c = \emptyset$ · $\emptyset^c = U$
12	Set difference	$A - B = A \cap B^c$

Reproduced with worked proofs in proving-set-properties[72].

Note the one-to-one correspondence with the logical equivalences in block 1 — laws 1–11 are those same eleven laws in the same order, plus set difference at 12. The names are not quite identical: *negation* becomes **complement** (5), *double negative* becomes **double complement** (6), and *negations of* **t** *and* **c** becomes **complement of** U **and** $\emptyset$ (11). That correspondence is not a coincidence: $\cup$ behaves as $\vee$, $\cap$ as $\wedge$, and complement as $\sim$. Law 12 is the one with no counterpart in block 1.

The numbering is not decoration — it is how the course expects you to cite. The worked identity proof in Lecture 18 justifies its lines by the number on this page: *by set diff law (12)*, *by de Morgan (9b)*, *dist. law (3b)*, *complement law (5b)*, *identity law (4a)* — only the double complement step goes uncited there, by name alone. Naming and numbering the law is where the marks are, and this page is in front of you while you do it.

4. The Quotient-Remainder Theorem

> Given any integer n and any positive integer d, there exist **unique** integers q and r such that $n = dq + r$ and $0 \leq r < d$.

[72] courses/math1061/proving-set-properties.pdf

See modular-arithmetic[73]. The uniqueness clause and the range $0 \leq r < d$ are what let you read a remainder off a rearranged expression.

5. Unique Factorisation Theorem

> Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that
>
> $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
>
> and **any other expression for n as a product of prime numbers is identical to this except perhaps for the order** in which the factors are written.

See divisibility-and-factorisation[74]. The second half is the "unique" part, and it is the half students leave out when asked to state the theorem.

6. Schröder-Bernstein Theorem

> For all sets A and B, if $|A| \leq |B|$ and $|A| \geq |B|$ then $|A| = |B|$.

See cardinality[75]. In use it means two injections, one each way, in place of one bijection, and the two must point in opposite directions between the same two sets.

7. Binomial Theorem

> Given any real numbers a and b, and any nonnegative integer n,
>
> $$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Belongs to the counting material (L30–L31). The coefficient $\binom{n}{k}$ is "n choose k", the number of k-element subsets of an n-element set (counting-selections[76]). The theorem, with its proof by counting a, b-sequences and the method for picking one coefficient out of an expansion, is in binomial-coefficients[77].

---

[73] courses/math1061/modular-arithmetic.pdf
[74] courses/math1061/divisibility-and-factorisation.pdf
[75] courses/math1061/cardinality.pdf
[76] courses/math1061/counting-selections.pdf
[77] courses/math1061/binomial-coefficients.pdf

What this means for revision

Blocks 1 and 2 are the bulk of the page and are reproduced in the vault, so for the logic material the assessed skill is **recognising and naming** which law or form applies — not recalling the list.

Block 3 works the same way: the set identities are given, so the assessed skill is choosing and **citing by number**, not reciting the twelve laws — see proving-set-properties[78] for both worked methods that use them.

Blocks 4 and 5 are covered by modular-arithmetic[79] and divisibility-and-factorisation[80]. Block 6 is covered by cardinality[81]. Block 7 is covered by binomial-coefficients[82], and its $\binom{n}{k}$ by counting-selections[83].

Nothing else is provided. In particular the whole of set theory apart from block 3 — the definitions of $\subseteq$, $\subset$, $\mathcal{P}(A)$, $A \times B$, partition, function, image and preimage — is **not** on the page, and neither is any proof technique, nor anything about sequences, induction and recursion. Nor is anything about relations, groups or fields: the definitions of reflexive, symmetric, transitive and antisymmetric, of an equivalence relation (equivalence-relations[84]) and a partial order (partial-order-relations[85]), the four group properties (groups[86]), the subgroup checks (subgroups-and-cyclic-groups[87]) and the conditions for a field (fields[88]). Nor are the counting rules and selection formulas of counting-principles[89] and counting-selections[90], Pascal's formula, inclusion/exclusion (inclusion-exclusion[91]), the pigeonhole principle (pigeonhole-principle[92]) or the Handshake Theorem ([graphs]). Nor is any of the rest of the graph theory: the definitions of walk, trail, circuit and connected (walks-trails-and-circuits[93]), the Euler circuit and trail theorem (euler-circuits-and-trails[94]), adjacency and incidence matrices (adjacency-matrices[95], incidence-matrices[96]), or the theorem that a tree with n vertices has $n-1$ edges (trees[97]). All

[78] courses/math1061/proving-set-properties.pdf
[79] courses/math1061/modular-arithmetic.pdf
[80] courses/math1061/divisibility-and-factorisation.pdf
[81] courses/math1061/cardinality.pdf
[82] courses/math1061/binomial-coefficients.pdf
[83] courses/math1061/counting-selections.pdf
[84] courses/math1061/equivalence-relations.pdf
[85] courses/math1061/partial-order-relations.pdf
[86] courses/math1061/groups.pdf
[87] courses/math1061/subgroups-and-cyclic-groups.pdf
[88] courses/math1061/fields.pdf
[89] courses/math1061/counting-principles.pdf
[90] courses/math1061/counting-selections.pdf
[91] courses/math1061/inclusion-exclusion.pdf
[92] courses/math1061/pigeonhole-principle.pdf
[93] courses/math1061/walks-trails-and-circuits.pdf
[94] courses/math1061/euler-circuits-and-trails.pdf
[95] courses/math1061/adjacency-matrices.pdf
[96] courses/math1061/incidence-matrices.pdf
[97] courses/math1061/trees.pdf

of that has to come from memory.

Graphs

A graph is a set of points, the vertices, with some of them joined by lines, the edges. Almost all of graph theory is built on the few definitions here: what a graph is, loops and multiple edges, simple graphs, and the degree of a vertex. Then the first theorem, the Handshake Theorem, which says the degrees always add up to twice the number of edges, and what follows from it: every graph has an even number of vertices of odd degree, and many lists of numbers cannot be the degrees of any graph. The pigeonhole argument that two vertices of a simple graph share a degree is in pigeonhole-principle[98]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[99]. What comes after builds on these: getting around a graph (walks-trails-and-circuits[100]), using every edge exactly once (euler-circuits-and-trails[101]), writing a graph as a matrix (adjacency-matrices[102], incidence-matrices[103]), and the connected graphs with no circuits (trees[104]).

What a graph is

> A **graph** G is a non-empty set of **vertices** $V(G)$ and a (possibly empty) set of **edges** $E(G)$, where each edge is associated with a set consisting of either one or two vertices.

The vertices an edge is associated with are its **endpoints**. An edge with two endpoints joins them, and an edge with one endpoint joins that vertex to itself.

- A graph must have **at least one vertex**, but it may have **no edges at all**.
- An edge is an object in its own right, not just a pair of vertices. Two different edges can have the same endpoints, and that is why edges are given their own names, $e_1, e_2, \ldots$.

Two standard words: two vertices joined by an edge are **adjacent**, and an edge is **incident** with each of its endpoints. A vertex with no edges at all is **isolated**.

Drawing a graph. Each vertex is a dot and each edge a line between the dots of its endpoints, or a small loop from a dot back to itself. The graph is only the vertices, the edges and which edges have which endpoints. Where the dots go, and whether the lines are straight or curved, carry no information, so the same graph can be drawn in many ways. Two lines that cross in a drawing do not meet at a vertex; only dots are vertices.

[98] courses/math1061/pigeonhole-principle.pdf
[99] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[100] courses/math1061/walks-trails-and-circuits.pdf
[101] courses/math1061/euler-circuits-and-trails.pdf
[102] courses/math1061/adjacency-matrices.pdf
[103] courses/math1061/incidence-matrices.pdf
[104] courses/math1061/trees.pdf

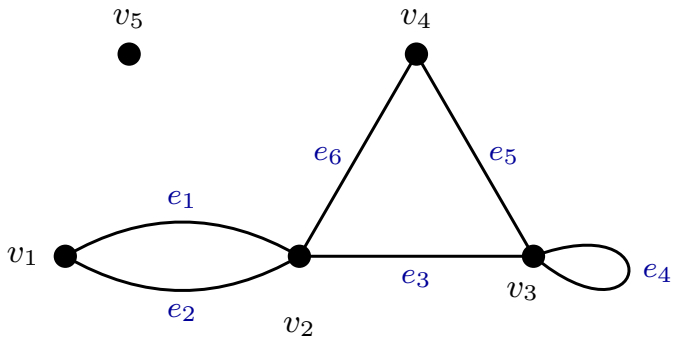


Figure 13: A graph with vertices v_1 to v_5 and edges e_1 to e_6. The edges e_1 and e_2 have the same endpoints, v_1 and v_2, so they are multiple edges. The edge e_4 has the single endpoint v_3, so it is a loop. v_5 is an isolated vertex: no edge has it as an endpoint, but it is still part of the graph. The edge e_6 joins v_2 and v_4, so those two vertices are adjacent and e_6 is incident with each of them; v_1 and v_3 are not adjacent, since no edge joins them. The graph is not simple, because of the loop and because of the multiple edges.

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_2\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_3\}$
e_5	$\{v_3, v_4\}$
e_6	$\{v_2, v_4\}$

The table is the graph. The drawing is one picture of it.

Loops and multiple edges

- A **loop** is an edge with only one endpoint. It joins a vertex to itself. Above, e_4 is a loop at v_3.
- **Multiple edges** (also called **parallel edges**) are two or more edges with the same set of endpoints. Above, e_1 and e_2 both join v_1 and v_2.

Both come up naturally when a graph models something. In the bridges of Königsberg, two

land masses are joined by two bridges, which gives multiple edges (2026-07-27-welcome-and-intro-problems[105]).

Simple graphs

> A graph is **simple** if it has no loops and no multiple edges.

In a simple graph every edge has two different endpoints, and two vertices are joined by at most one edge. So an edge can be named by its endpoints, and a simple graph is just a set of vertices with some pairs of them joined.

A simple graph with n vertices has every degree at most $n-1$. A vertex can be joined to each of the other $n-1$ vertices at most once, and not to itself. This bound is one of the two quick tests for degree sequences.

Degree

> The **degree** of a vertex v, written $\deg(v)$, is the number of edge ends incident with it.

Count the ends of edges at the vertex, not the edges.

- An ordinary edge has one end at each of its two endpoints, so it adds 1 to the degree of each.
- **A loop has both of its ends at the same vertex, so it adds 2** to the degree of that vertex.
- An isolated vertex has degree 0.

In the graph above:

Vertex	Edge ends at it	Degree
v_1	e_1, e_2	2
v_2	e_1, e_2, e_3, e_6	4
v_3	e_3, e_4 twice, e_5	4
v_4	e_5, e_6	2
v_5	none	0

The degrees add to $2+4+4+2+0=12$, and there are 6 edges.

Why a loop counts 2: degree counts the ways out of a vertex along an edge. A loop can be set off along in either direction, so it gives two ways out. Counting it as 2 is also what makes the Handshake Theorem hold for every graph.

[105] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

The Handshake Theorem

The Handshake Theorem. The sum of the degrees of a graph is twice the number of edges. If G is a graph with $V(G) = \{v_1, v_2, \ldots, v_n\}$ and $|E(G)| = e$, then

$$\sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2e.$$

Proof. Count the edge ends in the graph two ways. Every edge has exactly two ends: an edge with two endpoints has one at each, and a loop has both at its one endpoint. So there are $2e$ ends in all. Every end is at exactly one vertex, and $\deg(v_i)$ is the number of ends at v_i. So adding the degrees over all the vertices counts each end exactly once, and the sum is $2e$. □

The name comes from people shaking hands at a party. Each handshake involves two hands, so the total number of hands shaken, added up person by person, is twice the number of handshakes.

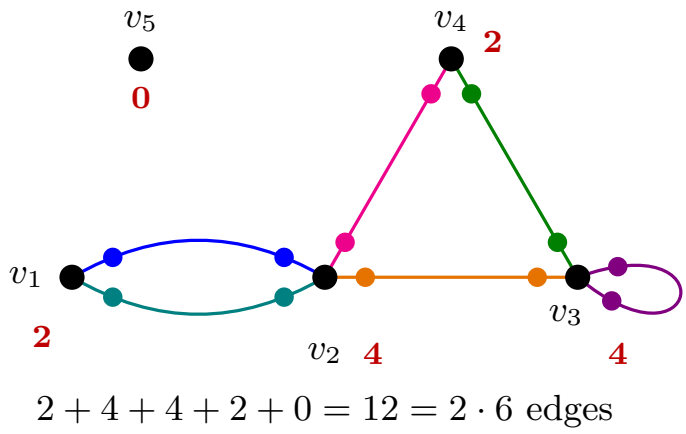


Figure 14: The proof of the Handshake Theorem, on the graph above. Every edge is drawn in its own colour, with a dot of that colour at each of its two ends. The loop e_4 has both of its dots at v_3. The degree of a vertex is the number of dots at it, so adding up the degrees counts every dot once. Each edge has exactly two dots, so the 6 edges give 12 dots, and the degrees add to 12.

Using it. The theorem links the degrees to the number of edges, so either can be found from the other.

- **Number of edges from the degrees.** A graph with degrees $4, 4, 3, 3, 2, 2$ has $\frac{18}{2} = 9$ edges.

- **No graph with an odd degree sum.** There is no graph with 7 vertices each of degree 3: the degrees would add to 21, and 21 is not $2e$ for any whole number e. More generally, if every vertex has degree 3 then $3n = 2e$, so the number of vertices n must be even.
- **Edges of a complete graph**, below.

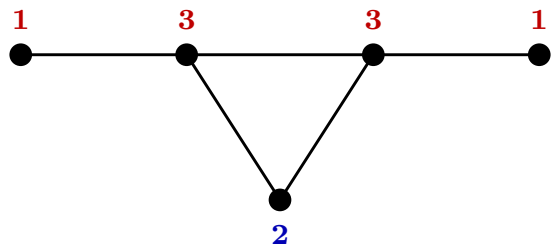
Odd-degree vertices come in pairs

Corollary. Every graph has an even number of vertices of odd degree.

Proof. Split the sum of the degrees into the vertices of even degree and the vertices of odd degree:

$$\underbrace{\sum_{\deg(v)\text{ even}} \deg(v)}_{\text{even}} + \sum_{\deg(v)\text{ odd}} \deg(v) = 2e.$$

The first sum is a sum of even numbers, so it is even. The right side is even. So the second sum, being the difference of two even numbers, is even. It is a sum of odd numbers, and a sum of odd numbers is even exactly when there is an even number of terms: odd numbers pair up into even sums, and one left over makes the total odd. So the number of vertices of odd degree is even. □



$$\underbrace{2}_{\text{even}} + \underbrace{(3+3)+(1+1)}_{\text{odd degrees, in pairs}} = 10 = 2 \cdot 5 \text{ edges}$$

Figure 15: The corollary on a graph with degrees 3, 3, 2, 1, 1, odd degrees in red and even in blue. The degree sum is $2e = 10$, even. Its even part, 2, is even, so its odd part, $3+3+1+1$, must be even as well. A sum of odd numbers is even only when the odd numbers pair off, each pair adding to an even number. Here the four odd degrees make two pairs. A fifth vertex of odd degree would be left without a partner and make the total odd, which no graph allows.

The corollary says nothing about the vertices of **even** degree. Their number can be odd or even: one vertex joined to four others has one vertex of even degree, and a path of four vertices has two. That is worked as a multiple-choice question in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[106].

In practice the corollary is the quickest check on a list of degrees: **count the odd entries**. If there is an odd number of them, no graph has those degrees.

Degree sequences

> The list of the degrees of the vertices in a graph is called the **degree sequence** of the graph.

It is usually written largest first. The graph above has degree sequence $4, 4, 2, 2, 0$. Only the list of numbers matters, not which vertex has which.

The usual question runs the other way: given a list, is there a graph, often a **simple** graph, with exactly those degrees? Two checks rule a list out:

1. **The sum must be even**, by the Handshake Theorem. Equivalently, the number of odd entries must be even. This holds for every graph.
2. **For a simple graph with n vertices, no entry can be more than $n-1$.** A list of n numbers with an entry of n or more has no simple graph.

These checks are necessary, not sufficient. A list can pass both and still have no simple graph. Take $3, 3, 3, 1$. The sum is 10, which is even, and no entry is more than $n - 1 = 3$. But with 4 vertices, a vertex of degree 3 in a simple graph is joined to all three others. There are three such vertices, and each of them is joined to the fourth vertex, which therefore has degree 3, not 1. So no simple graph has degree sequence $3, 3, 3, 1$.

So, after the two checks, a list that passes either gets a drawing or an argument like this one. Small cases can be settled by hand, building the graph from the vertex of largest degree down. A complete test for when a list is the degree sequence of a simple graph does exist (the Havel–Hakimi and Erdős–Gallai theorems), but it is beyond this course.

Without the word "simple", the answer is easy. If loops are allowed, **every list with an even sum is the degree sequence of some graph**. The odd entries come in an even number, so pair them up and join each pair by an edge. Now every vertex still needs an even number of edge ends, and a loop supplies 2, so add loops until each vertex has its degree. For example, $3, 2, 1$ has no simple graph, since degree 3 is impossible with only 3 vertices, but a graph with multiple edges has those degrees (2026-10-22-pigeonhole-principle-introduction-to-graph-theory[107]).

[106] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[107] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

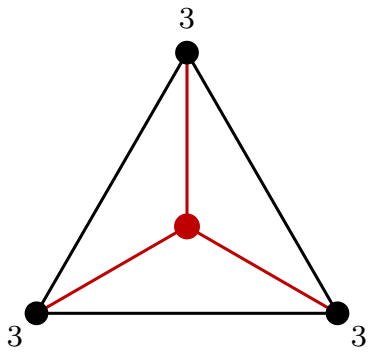


Figure 16: Why no simple graph has degree sequence 3, 3, 3, 1. In a simple graph on 4 vertices, a vertex of degree 3 is joined to every other vertex. The three vertices that need degree 3, black, must each be joined to the fourth vertex, red, which is then forced to have degree 3 as well. The list passes both quick checks, an even sum and no degree above 3, and still has no simple graph.

Worked: which lists are degree sequences

For each list, is there a simple graph with those degrees?

List	Sum	Largest vs $n-1$	Simple graph?
$2, 2, 2, 2$	8	$2 \leq 3$	yes: a square
$3, 2, 1$	6	$3 > 2$	no: too large
$4, 3, 2, 2, 2, 2, 1, 1$	17	$4 \leq 7$	no: odd sum (three odd entries)
$1, 1, 1, 1$	4	$1 \leq 3$	yes: two edges with no common vertex
$5, 5, 5, 5, 5, 5$	30	$5 \leq 5$	yes: the complete graph K_6
$3, 3, 3, 1$	10	$3 \leq 3$	no: passes both checks, fails as shown
$4, 4, 3, 3, 2, 2$	18	$4 \leq 5$	yes: 9 edges

The first five are drawn in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[108]. For the last, name the vertices a, b, c, d, e, f with the degrees in that order, and take the edges $ac, ad, ae, af, bc, bd, be, bf, cd$. Then a and b are each joined to c, d, e, f; c and d to a, b and each other; and e and f to a and b.

[108] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Complete graphs

The **complete graph** K_n is the simple graph with n vertices in which every pair of different vertices is joined by an edge. It is the standard name for this graph. Every vertex is joined to the other $n-1$, so every degree is $n-1$, the most a simple graph allows. K_6 is the graph with degree sequence $5, 5, 5, 5, 5, 5$.

How many edges? By the Handshake Theorem,

$$n(n-1) = 2e, \qquad \text{so} \qquad e = \frac{n(n-1)}{2}.$$

Or count directly: an edge of K_n is a choice of 2 of the n vertices, so there are $\binom{n}{2} = \frac{n(n-1)}{2}$ edges (counting-selections[109]). The two counts agree. K_6 has $\frac{6 \cdot 5}{2} = 15$ edges.

$\binom{n}{2}$ is the most edges a simple graph on n vertices can have. Each edge of a simple graph is a different pair of vertices, and there are only $\binom{n}{2}$ pairs. K_n uses every pair, so it is the only simple graph on n vertices that reaches the bound.

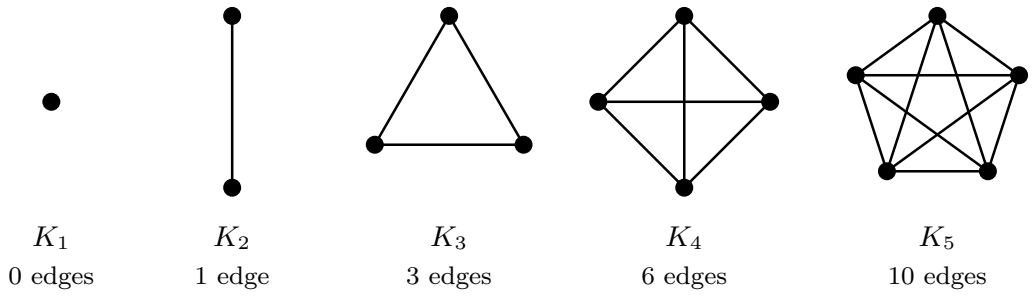


Figure 17: The complete graphs K_1 to K_5, each with every pair of vertices joined. Each vertex of K_n has degree $n-1$, so the degrees add to $n(n-1)$ and there are $\frac{n(n-1)}{2}$ edges: 0, 1, 3, 6 and 10. In K_4 and K_5 some lines cross where there is no vertex. Only the dots are vertices.

Common mistakes

- **Counting a loop once.** A loop adds 2 to the degree of its vertex. Counting it as 1 makes the degree sum odd and breaks the Handshake Theorem.
- **Treating a crossing as a vertex.** Lines that cross in a drawing are not joined. A vertex is a dot.

[109] courses/math1061/counting-selections.pdf

- **Taking an even sum as enough.** The Handshake Theorem rules a list out when its sum is odd, but an even sum does not make a simple graph exist: $3, 2, 1$ and $3, 3, 3, 1$ both have even sums and no simple graph.
- **Forgetting the word "simple".** Without it, loops and multiple edges are allowed, and any list with an even sum has a graph. With it, every degree is at most $n - 1$.
- **Mixing up the corollary.** The number of vertices of **odd** degree is always even. The number of vertices of even degree can be anything.
- **Reading the drawing as the graph.** Where the dots are and how the lines bend do not matter. The graph is the vertices, the edges and their endpoints.

See also

- pigeonhole-principle[110] — every simple graph with at least two vertices has two vertices of equal degree
- counting-selections[111] — $\binom{n}{2}$, the number of edges of K_n
- 2026-07-27-welcome-and-intro-problems[112] — the bridges of Königsberg as a graph
- walks-trails-and-circuits[113] — walks, trails, circuits and connected graphs
- euler-circuits-and-trails[114] — when a graph can be traced using every edge exactly once
- adjacency-matrices[115] · incidence-matrices[116] — a graph written as a matrix
- trees[117] — connected graphs with no circuits
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[118] — Lecture 33
- 2026-10-26-walks-trails-and-circuits[119] — Lecture 34, which recaps these definitions
- practice-problems[120] — §43, with full worked solutions

Logical Connectives

Logic is the study of reasoning, and the language of symbolic logic is what lets us **analyse ordinary sentences**, **test arguments for validity**, **construct proofs for complex arguments**, and **identify incorrect proofs and common fallacies**. This note covers the first layer of that language: statements, the three basic connectives, and the truth tables that define them.

[110] courses/math1061/pigeonhole-principle.pdf
[111] courses/math1061/counting-selections.pdf
[112] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[113] courses/math1061/walks-trails-and-circuits.pdf
[114] courses/math1061/euler-circuits-and-trails.pdf
[115] courses/math1061/adjacency-matrices.pdf
[116] courses/math1061/incidence-matrices.pdf
[117] courses/math1061/trees.pdf
[118] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[119] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[120] courses/math1061/practice-problems.pdf

Statements

A **statement** (or **proposition**) is a sentence that is either true or false, but not both. Represented by variables $p, q, r, ...$

Sentence	Statement?	Why
"6 is odd."	**Yes** — and it is false	Definitely one of T/F, and we can say which
"It is raining."	**Yes**	Which value it takes depends on the circumstances — it could be either — but in any given circumstance it is definitely one or the other
"x is odd."	**No**	Its truth depends on the unspecified x, so it has no truth value on its own
"Is it raining?"	**No**	A question is not true or false
"She is happy."	**No**	Not objectively true or false

The row worth pausing on is "It is raining." A sentence does not stop being a statement just because you personally don't know which value it has. What disqualifies "x is odd." is different: it has a **free variable**, so there is nothing to be true *about* until x is fixed. Sentences of that shape are **predicates**, and the machinery for turning them into statements is quantifiers — see quantified-statements[121].

Basic connectives

Connective	Symbol	Alt. symbol
not	$\sim$	$\neg$
and	$\wedge$	
or (inclusive)	$\vee$	

$\sim$ and $\neg$ are both common symbols for "not". **This course writes** $\sim$, and so does the examination formula page, so that is what these notes use.

$p \vee q$ is true when p is true, q is true, or both ("inclusive or").

[121] courses/math1061/quantified-statements.pdf

The defining truth tables

These three must be known by heart:

p	q	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

p	$\sim p$
T	F
F	T

Inclusive vs exclusive in English

Ordinary English uses "or" both ways:

- *"Would you like red or white wine?"* — reads as **exclusive**; you're expected to pick one.
- *"Would you like milk or sugar with your tea?"* — reads as **inclusive**; both is a perfectly good answer.

$\vee$ is always the inclusive one.

Translating English into symbols

Translating between English and mathematics is difficult, and three English words carry most of that difficulty:

English	Symbolic	Note
but	$\wedge$	Carries a contrast in English, none in logic — "it is not cold **but** it is snowing" is $\sim p \wedge q$
neither A **nor** B	$\sim (A \vee B)$, equivalently $\sim A \wedge \sim B$	"Neither … nor" is *the negation of an "or" statement* — the De Morgan rewrite is why the two forms agree (see logical-equivalence-laws[122])

[122] courses/math1061/logical-equivalence-laws.pdf

English	Symbolic	Note
or	$\vee$	Always inclusive, whatever the English suggests

Worked. Let p = "it is cold", q = "it is snowing", r = "it is sunny".

English	Symbolic
It is not cold but it is snowing.	$\sim p \wedge q$
It is neither snowing nor cold, but it is sunny.	$\sim (q \vee p) \wedge r \ \equiv \ (\sim q \wedge \sim p) \wedge r$

and back the other way:

Symbolic	English
$\sim q \wedge p$	It is not snowing and it is cold.
$(p \wedge q) \vee r$	It is cold and snowing, **or** it is sunny. (Inclusive — a cold, snowing, sunny day satisfies it.)

Are "It is not cold but it is snowing" and "It is snowing and it is not cold" equivalent? Yes, by the **commutative law**: $\sim p \wedge q \equiv q \wedge \sim p$. The English word order changes and the meaning does not.

Exclusive or ($\oplus$)

"One or the other, but not both", often written **XOR**:

$$p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$$

Laid beside the two inclusive connectives, so the differences are visible in one place:

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

$\oplus$ is equivalent to neither of them:

$$p \oplus q \not\equiv p \vee q \qquad\qquad p \oplus q \not\equiv p \wedge q$$

$\oplus$ agrees with $\vee$ everywhere **except** the "both" row, and agrees with $\wedge$ **only** on the row where neither holds.

Order of operations

1. $\sim$ first.
2. $\wedge, \vee$ equal second — parenthesise, else left to right.

$\rightarrow$ and $\leftrightarrow$ join as an equal third tier; see conditional-statements[123].

Worked. Take the statement form

$$(p \wedge q) \vee \sim (r \vee p) \wedge s$$

Because $\sim$ binds first, the $\sim$ takes only $(r \vee p)$; the remaining $\vee$ and $\wedge$ are then resolved left to right. So it means

$$\big((p \wedge q) \vee (\sim (r \vee p))\big) \wedge s$$

which is a different statement form from $(p \wedge q) \vee \big((\sim (r \vee p)) \wedge s\big)$ — the reading you would get by assuming $\wedge$ binds tighter than $\vee$. In this course they are equal in precedence, so that assumption is wrong here. **Write the parentheses.**

Truth tables

A truth table shows the truth value of a statement form for **all possible** truth values of its statement variables. A statement form with n variables has 2^n rows, where n **counts the *distinct* letters**, not the occurrences.

Take $(p \wedge q) \wedge (q \wedge r)$. Each unique letter is a variable, so there are **3** variables p, q, r — not 2 and not 4 — and the table has $2^3 = 8$ rows. The repeated q does not add one.

[123] courses/math1061/conditional-statements.pdf

Standard truth table form

> Construct your truth tables in **standard form** so that (i) you are sure you have covered all combinations of the truth values of the statement variables, and (ii) it is easy for someone to check your work.

Standard form fixes the row order: the **first** variable is T for the whole top half and F for the whole bottom half, and each later variable halves the run again, so the **last** variable alternates T, F every row.

p	Statement form
T	
F	

$2^1 = 2$ rows

p	q	Statement form
T	T	
T	F	
F	T	
F	F	

$2^2 = 4$ rows

p	q	r	Statement form
T	T	T	
T	T	F	
T	F	T	
T	F	F	
F	T	T	
F	T	F	
F	F	T	
F	F	F	

4 2 1

$2^3 = 8$ rows

each column's run of like values halves: 4, 2, 1 — the last variable alternates every row

Figure 18: Standard truth table form for one, two and three variables. Each new variable doubles the number of rows and halves the run of like values — 4, 2, 1 for three variables — so the pattern is fixed and completeness is checkable at a glance. The rings mark that pattern on the three-variable table. The narrow amber column separates the variables from the statement-form column.

The four-variable table extends the same pattern: p runs T for eight rows then F for eight, q in blocks of four, r in blocks of two, s alternating — $2^4 = 16$ rows.

For how to *build* the intermediate columns of a compound form, and the convention of numbering them in evaluation order, see the worked table in 2026-07-30-logical-form-and-equivalence[124].

See also

- logical-equivalence-laws[125]

[124] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[125] courses/math1061/logical-equivalence-laws.pdf

- conditional-statements[126]
- quantified-statements[127] — what to do with sentences like "x is odd" that are not statements
- 2026-07-30-logical-form-and-equivalence[128] — Lecture 2, where all of this was introduced
- practice-problems[129] — §1 Logical Form, with full worked solutions

Logical Equivalence & Laws

Two statement forms are **logically equivalent** ($\equiv$) if they have the same truth value for every combination of truth values of their variables — shown via a truth table, or by chaining the laws below. To show two forms are **not equivalent** ($\not\equiv$), exhibit one combination of truth values where they differ.

$\equiv$ *compares* statements (like $=$ compares numbers); it's not a connective itself. The connective that *combines* two statements into one is the biconditional $\leftrightarrow$ — see conditional-statements[130].

Tautologies and contradictions

> A **tautology t** is a statement that is **always true**. A **contradiction c** is a statement that is **always false**.

Both are written in bold upright lower case on the formula sheet, and both appear as *values* inside the laws — $p \vee \sim p \equiv \mathbf{t}$ produces one, $p \wedge \mathbf{t} \equiv p$ consumes one. A chain of laws that reaches **t** or **c** has proved the original form is always true or always false, which is usually the point of the exercise.

Laws of logical equivalence

> **Provided in the exam.** These laws are printed on the *MATH1061/MATH7861 Examination Formula Page*, so they don't need memorising. What the exercises ask for is choosing and applying them, and naming the one used at each step. The same page also carries the valid-argument-forms[131] and the set identities of proving-set-properties[132].

[126] courses/math1061/conditional-statements.pdf
[127] courses/math1061/quantified-statements.pdf
[128] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[129] courses/math1061/practice-problems.pdf
[130] courses/math1061/conditional-statements.pdf
[131] courses/math1061/valid-argument-forms.pdf
[132] courses/math1061/proving-set-properties.pdf

Given statement variables p, q, r, a tautology $\mathbf{t}$, and a contradiction $\mathbf{c}$:

Law	Form 1	Form 2
Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negation	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
Double negative	$\sim (\sim p) \equiv p$	
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
De Morgan's	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negations of $\mathbf{t}/\mathbf{c}$	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

De Morgan's Laws are especially important for negating "and"/"or" statements — e.g. the negation of "5 is divisible by 2 **and** 6 is divisible by 2" is "5 is **not** divisible by 2 **or** 6 is **not** divisible by 2". Note what changes: the connective flips from *and* to *or*, and **both** halves get negated. Negating only one half, or leaving the connective alone, is the standard error.

How to write a law chain

The layout expected in your own work:

- the **first line is the starting expression**, on its own;
- **every later line begins with** $\equiv$, vertically aligned down the page;
- the **name of the law** used to get there sits in its own **right-hand column** on that line.

Two or more laws may be cited on one line if they act on the same step (e.g. "by De Morgan's law and the double negative law"). Name a law on every line that *changes* the expression. The one kind of line that goes unnamed is a pure re-labelling that asserts nothing new, like the "where $r = (p \wedge \sim q)$" line in the first worked example below.

Treat a compound expression as a single letter

The laws are stated for variables p, q, r, but they hold with **any statement form** substituted in. Spotting that turns a long expression into a short one:

$$(p \wedge \sim q) \wedge \ \sim (p \wedge \sim q)$$

is $r \wedge \sim r$ with $r = (p \wedge \sim q)$, so the negation law applies directly and it is $\mathbf{c}$. This is exactly the move in the first worked example below.

Worked: reaching a contradiction

Show that $(p \wedge \sim q) \wedge (\sim p \vee q) \equiv \mathbf{c}$**.**

$$\begin{aligned}
(p \wedge \sim q) \wedge (\sim p \vee q) &\equiv (p \wedge \sim q) \wedge \ \sim (p \wedge \sim q) && \text{by De Morgan's law and the double negative law} \\
&\equiv r \wedge \sim r \quad \text{where } r = (p \wedge \sim q) \\
&\equiv \mathbf{c} && \text{by the negation law}
\end{aligned}$$

The whole proof is the first line: recognising that $\sim p \vee q$ is $\sim (p \wedge \sim q)$ in disguise. Read De Morgan's backwards — $\sim p \vee q \equiv \sim p \vee \sim (\sim q) \equiv \sim (p \wedge \sim q)$ — and the two conjuncts are a statement and its own negation.

Worked: absorbing a conjunction

Show that $\sim p \vee (p \wedge q) \equiv \sim p \vee q$**.**

$$\begin{aligned}
\sim p \vee (p \wedge q) &\equiv (\sim p \vee p) \wedge (\sim p \vee q) && \text{by the distributive law} \\
&\equiv \mathbf{t} \wedge (\sim p \vee q) && \text{by the negation law} \\
&\equiv \sim p \vee q && \text{by the identity law}
\end{aligned}$$

The pattern *distribute, collapse the tautology or contradiction, drop it with the identity law* is the most common three-step shape in this topic, and it recurs in both routes below.

Worked: two routes to the same answer

Show that $\sim ((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \equiv p$**.**

There is no unique chain. Here are two, and both are complete proofs:

Neither route is "the" answer, and nothing turns on finding the short one. What matters is that every line follows from the one above by a **named** law. The shorter route is found by looking for a **common factor** before doing anything else: both disjuncts inside the brackets contain $\sim p$, so the distributive law pulls it out and the rest collapses.

The same equivalence can also be established with a truth table — see the worked table in 2026-07-30-logical-form-and-equivalence[133], where the column for $\sim ((\sim p \wedge q) \vee (\sim p \wedge \sim q))$ comes out identical to the column for p.

[133] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf

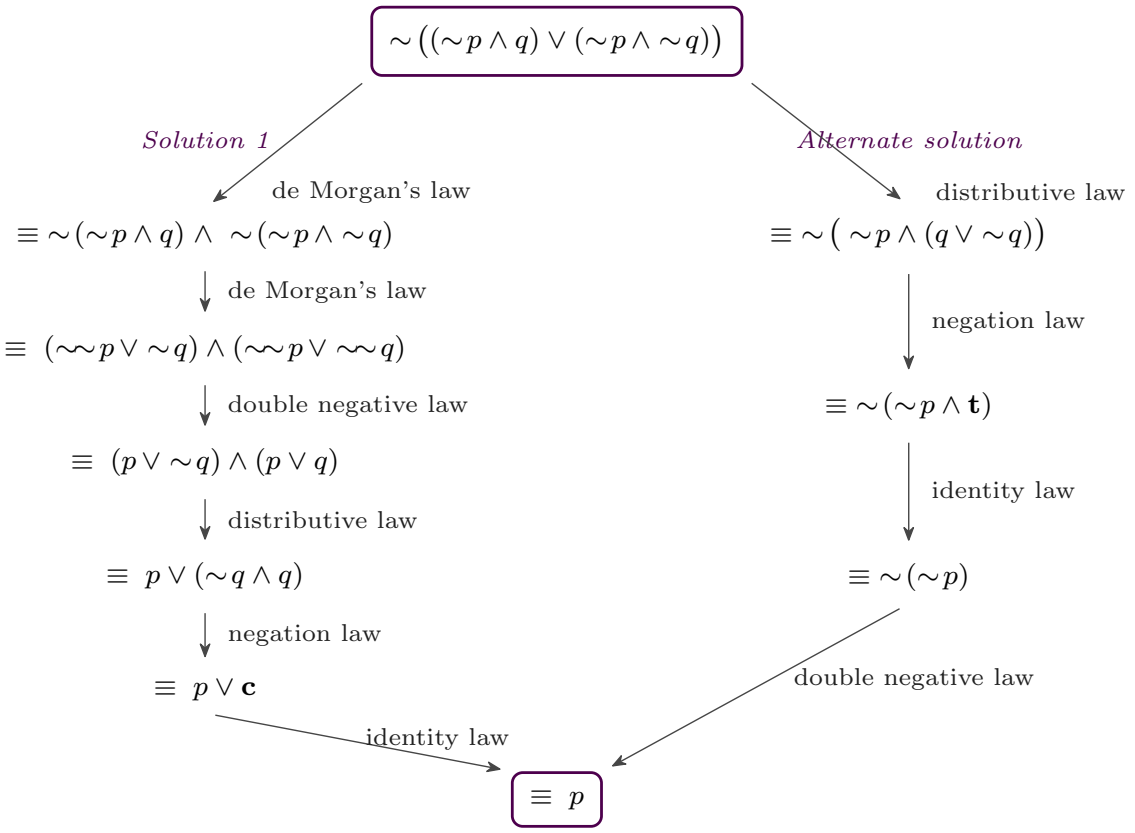


Figure 19: The same equivalence proved two ways. Starting from the same expression and ending at the same p, the left route pushes the negation inward with De Morgan's first and takes six steps; the right route factors out the common ~p with the distributive law first and takes four. Every edge names the law that licenses it — that naming is what the chain is for.

Showing two forms are *not* equivalent

To show $\not\equiv$ you do **not** need a full truth table. Find **one** assignment of truth values on which the two forms disagree, and say what each evaluates to.

Worked. Show that $\sim(p \vee q) \not\equiv \sim p \vee \sim q$.

Take p **false** and q **true**. Then

- LHS: $p \vee q$ is $\mathrm{F} \vee \mathrm{T} = \mathrm{T}$, so $\sim(p \vee q)$ is **false**.
- RHS: $\sim p \vee \sim q$ is $\mathrm{T} \vee \mathrm{F} = \mathrm{T}$, so it is **true**.

One row on which they differ is a complete disproof, so the two forms are **not** logically equivalent.

The correct partner for $\sim(p \vee q)$ is of course $\sim p \wedge \sim q$ — this is precisely the De Morgan trap of changing the sign but not the connective.

See also

- logical-connectives[134]
- conditional-statements[135]
- formula-sheet[136] — what else is provided in the exam, and what is not
- proving-set-properties[137] — the same eleven laws as set identities, and the two set-equality proof methods built on them
- 2026-07-30-logical-form-and-equivalence[138] — Lecture 2, where these laws were introduced and applied
- practice-problems[139] — §2 Logical Equivalence, with full worked solutions

Diagram and Notation Conventions

The house style for every figure, symbol and proof layout in MATH1061 — read off the course's own lecture slides rather than assumed. This is the authority any new diagram for this course is checked against. Where the source does not settle something, that is said so explicitly rather than filled in.

[134] courses/math1061/logical-connectives.pdf
[135] courses/math1061/conditional-statements.pdf
[136] courses/math1061/formula-sheet.pdf
[137] courses/math1061/proving-set-properties.pdf
[138] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[139] courses/math1061/practice-problems.pdf

What was read

Everything the course ships in the anchor set, in full: **all 176 slide pages across the 18 lecture decks (L01–L18), plus the 1-page examination formula sheet.** No sampling — the whole corpus was viewed as rendered images so the drawings, ink colours and box shapes were seen, not inferred from extracted text.

Citations below use `L07 p2` = **PDF page 2** of `math1061-lecture-07-…pdf`. Two decks have a page-label offset worth knowing: `L03 p2-p3` carry the printed header *Lecture 2*, and `L17 p9-p10` carry the printed header *Lecture 18*. PDF page position is what is cited.

The course ships one written reference — the *MATH1061/MATH7861 Examination Formula Page*. It is a genuine notation authority (it fixes , , bold **t**/**c**, `A` , , `A - B`, and the numbering of the set identities), but it is **not a drawing guide**: it says nothing about figures, colour, layout or symbol shape. Everything in the *Diagrams* section below is inferred from the decks alone.

Only **18 of the course's 36 lectures** exist in this set (L19–L36 — one-to-one/onto functions, composition, cardinality, relations, equivalence and partial orders, groups, fields, counting, probability, pigeonhole, graph theory, walks, matrix representations, trees — are absent). Conventions for those topics are unestablished; see the last section.

Provenance: two lecturers, one template

The course is split between two lecturers (`L01 p12`, course schedule): **Sara Davies** takes L01–L09 and L18–L26; **Katie Clinch** takes L10–L17 and L27–L36. Both use the same slide frame, but their annotation habits and some box conventions differ. Where they diverge it is recorded under Inconsistencies, not resolved.

Textbook lineage

The recommended text is **Susanna Epp, *Discrete Mathematics with Applications*, 4th or 5th (metric) edition** (`L01 p3`, with the cover image on the slide). It is cited repeatedly by page for statements and exercises — `L14 p7` ("Q27 on page 279 of Epp"), `L14 p8` ("Q31 on page 279"), `L16 p12` ("page 310 (in 4th edition) or page 346 (in 5th edition)"), `L18 p8` ("pages 419-421 (ed. 5) or pages 378-380 (ed. 4)").

Important qualification: no slide anywhere carries a caption naming a textbook as the source of a *figure*. The Epp lineage is real for wording and content — the logical-equivalence names, the valid-argument-form names and the twelve numbered set identities are Epp's — but it is **not** documented evidence for any drawing style. Do not cite Epp as a figure source.

Slide frame and page furniture

Element	Convention	Evidence	Holds?
Header band	Page 1 of each deck: `MATH1061/MATH7861 Discrete Mathematics Semester 2, 2026` at far left, `Lecture N - Title` at far right. Later pages: right-hand lecture label only. A full-width thin black rule sits beneath.	`L02 p1` vs `L02 p2`; identical in every deck L02–L18	Every deck except L01, which has UQ-branded title slides
Pre-work box	A **purple rounded-rectangle** box, top right of page 1, headed `Pre-work video:` / `Pre-work videos:` in bold, listing `Video NNN Title` with three-digit zero-padded numbers	`L02 p1`, `L03 p1`, `L05 p1`, `L07 p1`, `L10 p1`, `L13 p1`, `L16 p1`, `L18 p1`	All 17 decks L02–L18 — the single most consistent element in the course
Learning goals	Bold `Learning Goals` heading, numbered list `1. 2. 3.`	`L02 p1` … `L18 p1`	Every deck L02–L18 (L07 p1 uses an unnumbered list — the one exception)
Student Q&A	Bold blue heading `Student questions and comments:` (or `Student questions:`), questions in **blue**, answers in **red**	`L02 p1`, `L04 p1`, `L06 p1`, `L08 p1`, `L11 p1`, `L12 p1`, `L15 p1`, `L18 p1`	Every deck L02–L18

Element	Convention	Evidence	Holds?
Activities	Bold `Activity N:` restarting at 1 each lecture; pre-class items as `Q1 from the pre-class questions`; Clinch decks add `Poll question N:`	`L02 p3`, `L07 p5`, `L12 p2`, `L17 p3`	Throughout

Figures are **never numbered and never labelled "Figure"**. When a caption exists it sits centred directly beneath the drawing, either as the mathematical expression it depicts (`(A - B)`, `L18 p2`) or as a short prose verdict (`not a function` / `a function`, `L18 p9`).

Colour

Printed colour on slides

- **Red = the thing you must not get wrong.** Warnings, answers to student questions, "IMPORTANT NOTE", "Take care with notation!", "WARNING". `L01 p4` ("hurdles"), `L02 p1`, `L08 p2` ("WARNING"), `L10 p1` ("IMPORTANT NOTE"), `L11 p4` ("Take care with notation!"), `L17 p2` ("Warning!!!!"), `L17 p9`. Holds in both lecturers' decks, all semester.
- **Blue = student voice and explanatory gloss.** Student questions (`L02 p1` onward, universal) and, in Clinch's decks, a plain-English restatement placed *directly beneath* a formal condition written in red — `L12 p3` (`d|a and d|b` in red, "*d is a divisor of both a and b*" in blue below it), `L12 p4` (same pattern for lcm). That paired red-above/blue-below idiom is specific and recurs.
- **Colour as correspondence, not meaning.** Where two expressions must be matched piece-by-piece, matching pieces are given matching colours. `L03 p9` (a three-row table where `a  b`, `a if and only if b`, `b is necessary and sufficient for a` are colour-aligned column by column), `L06 p6` (quantifier negation, below), `L11 p3` (quotient in red above q, remainder in red above r, and the same two colours on the worked examples). This is the one place colour genuinely carries information.
- **Pastel highlight capsules** (yellow, green, blue, pink, orange) mark the single expression being tracked through a calculation — it keeps its capsule colour as it moves line to line. Heavily used by Clinch: `L11 p3`, `L12 p6`, `L13 p6`, `L14 p3`, `L16 p5`, `L17 p5`. Rare in Davies's decks.

Annotation ink (live handwriting)

Both lecturers annotate over the slides in ink. **Blue is the predominant ink for the main worked solution** — `L01 p13`, `L02 p7`, `L04 p4`, `L07 p4`, `L08 p5`, `L10 p5`, `L13 p7`, `L16 p7`, `L18 p3`. Other colours (green, red, purple, orange, teal) are layered over it for justifications, second solutions, and circling.

Be honest about what ink colour means: mostly, nothing fixed. It separates successive layers of annotation for legibility, and rotates. The two places it *is* systematic:

1. **Correspondence** — e.g. `L02 p6`, where each intermediate truth-table column is written in its own colour and numbered in that colour to show evaluation order, with the final column ringed and labelled "final answer".
2. **Verdict marks** — a green circled `T` and a red circled `F` for true/false answers: `L05 p7`, `L05 p8`, `L06 p4`. Green tick / red cross for correct/incorrect options: `L06 p3`, `L09 p4`, `L16 p2`.

Boxes and callouts

Shape	Meaning	Evidence	Holds?
Purple rounded rectangle	A named, quotable object: definition, Fact, Lemma, Theorem — and the pre-work video box	`L07 p1` (the six definitions), `L07 p2` (two Facts), `L08 p2`, `L09 p6` (Fact + Lemma), `L10 p6`, `L10 p7` (Unique Factorisation Theorem), `L10 p9`, `L10 p12`, `L11 p3` (Quotient-Remainder Theorem), `L11 p7`, `L11 p8`	Strong: both lecturers, L07 through L12
Plain thin black rectangle	A structural panel — a proof skeleton, or a two-way comparison	`L07 p3`, `L08 p3`, `L09 p2` (the four proof-method skeletons), `L11 p3` ("2 equivalent ways of defining…")	Consistent where it appears

Shape	Meaning	Evidence	Holds?
Red rectangle	Davies: a fact that must be memorised or a warning. Clinch: a numbered step caption or a named principle	`L02 p8` (De Morgan's laws), `L03 p4`, `L03 p9`, `L04 p1` ("Recall:"), `L01 p4`; and `L10 p6` (margin commentary), `L12 p10` (steps 1/2/3), `L14 p6` (Well-ordering Principle)	Both uses recur; see Inconsistencies
Margin callout with arrow	A red-outlined box in the right margin, with a red arrow to the exact proof line it explains, and a purple at the anchor point	`L10 p6` (two callouts, two arrows, two stars)	Seen once — extrapolating from a single instance
Hand-drawn cloud	An aside or a menu of options: "What type of proof will work?" with / against each method	`L09 p4`, `L09 p5`, `L09 p6`, `L09 p7`; `L14 p3`	Four consecutive slides in L09, once in L14

Logic notation

Fixed by the formula sheet and used unchanged in every deck:

Symbol	Reading	Note
`p`	not p	**The course symbol is the tilde , not ¬.** `L02 p1` answers this directly: "some common symbols for not include and ¬" — both exist, this course writes . Used in every deck and on the formula sheet
`p q`, `p q`	and, or	is **inclusive** or; exclusive or is (`L02 p5`)
`p → q`	if p then q	`L03 p1`; defined as `p q`

Symbol	Reading	Note
p q	if and only if	A **connective that combines** statements
p q, p q	logically equivalent / not	A **relation that compares** statements
t, **c**	tautology, contradiction	Bold upright, lower case. Formula sheet; L02 p9
	therefore	Prefixes the conclusion of an argument

versus is stated explicitly and must not be blurred (L03 p7): "The biconditional ( ) is a conjunction used to **combine** statements (similar to +, -, x, ÷ … with numbers). Logical equivalence ( ) is used when **comparing** two statements (similar to = with numbers)."

Precedence (L02 p5, extended at L03 p7): first; and equal second; → and equal third; within a tier, work left to right — "but parentheses should always be used to avoid confusion."

Statement variables are lower-case italic p, q, r. When a problem is in English, the letters are chosen as mnemonics of the English phrase: w = wages, b = buying, d = depression (L04 p4); q = queued, s = sent to the buffer (L05 p2).

Truth tables

The course calls this **"standard truth table form"** and requires it (L02 p4): *"You should construct your truth tables in standard form so that you are sure you have covered all combinations … and it is easy for someone to check your work."*

- **Values are the single upright capitals T and F** — never 1/0, never True/False. Universal: L02 p4, L03 p1, L04 p5, L06 p2, L07 p3, L09 p2.
- **2 rows for *n* variables**, in a fixed order: the first variable is T for the whole top half then F for the whole bottom half; each subsequent variable halves again; the last variable alternates T,F every row. Shown for n = 1, 2, 3, 4 side by side at L02 p4.
- **A narrow solid-filled amber/orange column separates the input block from the compound-form block.** L02 p4 (after the variable columns, before "Statement form"); L04 p5 (after the variables *and* their simple negations, before the premise and conclusion columns). Two instances, both lecturers' style aside — treat as the course's own table furniture.
- **Header row typeset in red italic maths** (p, q, p → q), body values in black upright. L03 p1, L03 p4, L04 p1, L04 p2, L04 p5, L07 p3, L08 p3, L09 p2. Consistent throughout Davies's decks; Clinch draws no printed truth tables.
- Full ruled grid — every cell bordered.

- **When built by hand, columns are added left to right in evaluation order and numbered beneath**, each in its own ink colour, with the answer column ringed. L02 p6, L03 p2. At L03 p2 the two columns that must match are marked with a beneath and the verdict written out: "Starred columns are identical so ((p q) (p q)) p".

Arguments and inference proofs

Argument form (formula sheet; L04 p2, L04 p3, L04 p6, L05 p2, L05 p4): premises stacked one per line, left-aligned; the conclusion on the last line prefixed by . **No horizontal rule above the conclusion.** Premises are numbered 1. 2. 3. and the line is left unnumbered.

Rules-of-inference proof (L04 p6, L04 p7, L05 p4): numbered lines down the left, the derived statement in the middle, and the **justification in its own right-hand column**, phrased as from by contraposition, from & by transitivity, by double negative law, by definition of →. The annotation at L04 p6 is emphatic: **"must write explanations!"**.

Equivalence-law chains (L02 p10, L03 p8, L18 p5, L18 p7): first line is the starting expression; every subsequent line begins with (or = for sets), vertically aligned, with the named law in a right-hand column — by de Morgan's law, by the negation law, by identity law. For set identities the numbered law from the formula sheet is cited: by set diff law (12), by de Morgan (9b), dist. law (3b), complement law (5b), identity law (4a) (L18 p7).

Biconditional proofs are marked by direction: and label the two halves (L12 p8). Two named methods, with a stated preference — Method 1, prove each direction separately, is annotated "**recommended method**"; Method 2, an iff chain, is annotated "**Be careful! Quicker method but easy to make a logical error**" (L12 p8, L12 p9).

Quantifiers

- x D, P(x) — universal, **comma** after the domain.
- x D such that P(x) — existential, the words **"such that"**, abbreviated **s.t.** (L06 p1, L05 p7).
- Both established at L05 p5 and used unchanged through L08 p1, L17 p3.
- reads "is an element of" / "belongs to"; "is not an element of" (L05 p5).
- Negation rules, stated as displayed equivalences at L08 p1: (x D such that P(x)) x D, P(x) and (x D, P(x)) x D such that P(x).

Number sets

Blackboard-bold, established at `L05 p1` and used unchanged to the end: , , , .

Irrational numbers are written ¯ — with an overbar (`L05 p1`, `L09 p1`, `L09 p3`, `L09 p6`). Not ; the equality = ¯ is written by hand at `L09 p1` as a gloss, but the barred form is what the printed slides use.

Restrictions are written as superscripts on the set symbol, in italic, not as subscripts and not as prose:

```
^even ^odd ^nonneg ^prime ^composite ^{>1} ^{ 2} ^{ 1}
```

Evidence: `L05 p1` (, ^even, ^nonneg), `L07 p2` (^even, ^odd, ^prime, ^composite, ^{ 1}, ^{>1}), `L07 p6` (^{ 2}), `L10 p12` (^{ 2}), `L17 p10` (,). Strong and semester-long.

Proof layout

The four methods each have a **fixed printed skeleton**, given verbatim on a repeated slide (`L07 p3`, `L08 p3`, `L09 p2` — the same panel, grown one box at a time as methods are introduced). Reproduce these wordings:

- **Direct proof** — `Let x  D and suppose P(x). … Hence Q(x).`
- **Disproof by counterexample** — `Let x = . Then x  D and P(x) is true. However, Q(x) is false.  So x is a counterexample and the statement is false.`
- **Proof by contradiction** — `Suppose the negation of x  D, P(x) → Q(x) is true. That is, suppose x  D such that P(x) is true but Q(x) is false. … Hence something that is obviously wrong… This is a contradiction, and we conclude that … is true.`
- **Proof by contraposition** — `We prove the contrapositive of x  D, P(x) → Q(x), namely that x  D, Q(x) → P(x).  Let x  D and suppose Q(x).  … Hence, P(x).`

Each box carries a red caption directly beneath it saying what it establishes: `Shows the statement is true.` / `Shows the statement is false.` (`L07 p3`, `L08 p3`).

Other layout facts:

- `Proof:` **label**, then the hypothesis line, then the working with = signs vertically aligned in a column, then a `Hence`/`Thus`/`So` conclusion. `L07 p4`, `L07 p5`, `L08 p5`, `L09 p3`, `L10 p5`.
- **Method comparison is a two-column layout** with bold centred headings — `Direct Proof` left, `Proof by contradiction` right (`L08 p5`, `L08 p6`); `Proof SMI` / `Proof MI` / `Proof WOP` (`L14 p7`, `L14 p8`).

- **Without loss of generality, spelled out then abbreviated WLOG** (L08 p8, L09 p5).
- **Case splits are labelled Case 1: / Case 2:** (L10 p6, L10 p12, L14 p5).
- **Every proof unfolds definitions.** The six definitions in the purple box at L07 p1 / L08 p2 are stated as **biconditionals using** — e.g. n is an even integer n = 2k for some integer k, d|n d 0 and n = dk for some integer k — because they are used in both directions.
- **Introduce a *new* variable for each new existential.** Annotated explicitly at L08 p6: "use a **new** variable!" where m = 2k+1 is followed by n = 2 +1.

End-of-proof mark

Printed proofs end with an **open square** : L07 p3, L07 p4, L08 p3, L09 p2, L10 p6, L10 p11, L10 p12.

Handwritten proofs end with either a hand-drawn open square (L07 p5, L08 p8, L09 p4, L09 p5, L09 p6) or a **double slash //** (L10 p5, L11 p6, L13 p7, L13 p9, L14 p10, L15 p5, L16 p7, L18 p3, L18 p7). At L11 p6 the lecturer writes an explicit legend of the acceptable marks: **// or QED**. Treat all four as sanctioned.

Contradiction mark

Davies writes ( ) — two arrows meeting — inline at the point the contradiction lands: L08 p3, L08 p5, L08 p6, L08 p7, L08 p8, L09 p6. Clinch instead uses a small crossed glyph inline, e.g. "(proof by)" for "proof by contradiction" (L14 p6, twice). See Inconsistencies.

Induction

The named-step skeleton is fixed and printed identically in five separate proofs:

```
Proof:  Let P(n) be the predicate  statement .
Basis step:        verify P(a)  … so P(a) is true.
Inductive step:   Prove that  k    with k  a, if P(k) is true, then P(k+1) is true.
Inductive hypothesis:  Suppose that k  a is an integer and that P(k) is true.
        LHS of P(k+1):  chain of = with the RHS reached
        Therefore P(k+1) is true.
Therefore, by  PMI / SMI ,  statement  for each integer n  a.
```

Evidence: L13 p6, L13 p8, L14 p3, L14 p7, L16 p6, L16 p8, L16 p10. Step labels are printed in **blue** at L13 p6 and in **red** at L14 p3/L14 p7.

- LHS / RHS are the standard abbreviations, and the two sides are named and worked separately: LHS of P(1): … RHS of P(1): … (L13 p6, L13 p7, L16 p7).
- The step where the hypothesis is used is annotated (by the inductive hypothesis) on the same line (L13 p6, L13 p7, L14 p3).
- Slides ask for the steps to be named: *"It is a good idea to list these explicitly in your proofs to help the reader to follow the proof"* (L13 p1).
- Multiple base cases are listed one per line when strong induction needs them (L14 p4, L15 p8).

Number-theory notation

- **Divides: d | n. Does not divide: d n** (slashed bar). L05 p7, L07 p1, L10 p1, L10 p10, L14 p8.
- Equivalent phrasings given at L10 p1: *d divides n*, *d is a divisor of n*, *d is a factor of n*, *n is a multiple of d*.
- **n mod d = r** (upright mod as a binary operator, no brackets) versus **m n (mod d)** (congruence, (mod d) bracketed after the statement). These are different things and the course flags it twice under a red heading Take care with notation! — L11 p3, L11 p4, recapped L12 p2.
- **gcd(a, b) and lcm(a, b)**, lower case, upright roman (L12 p3, L12 p4). At L12 p3 the alternative hcf(a,b) is written and then **struck through** — it is not this course's name.
- **Floor x and ceiling x** (L11 p2).
- **Standard factored form**: n = p ^{e } p ^{e } p_k^{e_k} with the primes in **increasing** order p < p < < p_k (L10 p7, annotated "increasing" at L10 p8).
- **Multiplication is a centred dot** · in printed slides: 2 · 3 · 5 · 7 · 11 p (L10 p11), 5859 = 1232 · 4 + 931 (L12 p6), 2 · 100 + 5 · 10 + 4 · 1 (L11 p8), 3 · 1 + 2 (L13 p6).

Sequences, sums and recurrences

- **Summation Σ with i = m below and n above**; index letters i, j, k; change of variable written as j = i + 1 (L13 p3, L13 p4, L13 p6).
- A recursive definition of a **sequence** requires two named parts: **a recurrence relation** and **initial conditions** (L15 p3, L16 p7, L16 p9).
- A recursive definition of a **set** requires three named parts: **Base**, **Recursion**, **Restriction** — always in that order, with the Restriction worded "Nothing is in B other than objects defined by the Base and the Recursion" (L15 p6, L15 p7).
- Verifying a guessed explicit formula has two named methods: **Method 1** (check the initial conditions and the recurrence relation — annotated "quicker") and **Method 2** (prove it by induction — annotated "rigorous"). L16 p4, used at L16 p5–L16 p10.

- `n!` with `0! = 1` by definition (`L15 p5`).

Set-theory notation

Notation	Meaning	Evidence
`x  A`	is an element of	`L17 p1`
`A  B`	is a subset of	`L17 p1`, `L17 p3`
`A  B`	is a **proper** subset of (and there is an element of B not in A)	`L17 p3` — the course does use strictly for proper
`A  B`, `A  B`	intersection, union; indexed forms `_{i=1}^{3} A` , `_{i=1}^{3} A`	`L17 p1`, `L17 p6`
`A - B`	set difference; **`A \ B` is stated to be equally acceptable**	`L17 p1` — answered directly: "Yes. `A - B` can be written as `A \ B`"
`A`	complement, superscript `c`	`L17 p1`, `L18 p1`, formula sheet
`(A)`	power set, calligraphic script `P`	`L17 p1`, `L17 p7`, `L17 p8`
`A × B`	Cartesian product; `×` also written ²	`L17 p1`, `L17 p9`
	empty set, also written `{ }`	`L17 p5`
`|A|`	cardinality	`L17 p7`, `L17 p9`
`{n  | n  2 (mod 8)}`	set-builder with a vertical bar	`L17 p3`, `L18 p2`
`[a, b]`	closed interval `{x  | a  x  b}`	`L17 p6`

Sets take capital italic letters (`A, B, C, S, T, D, E, R, X, Y`), the universal set is `U`, elements take lower case (`x, y, t`). `L17 p3`, `L18 p1`, `L18 p6`.

The / distinction is the course's flagged trap — a red `Warning!!!!` at `L17 p2` and the first learning goal of both L17 and L18. `2  {2}` (`L17 p2`); is false, is true (`L17 p1`, `L17 p2`).

Proof of set statements has three named methods (`L18 p4`): **the element method**, **using the laws of logical equivalence**, and **using set identities** (citing the formula sheet's numbering, as above).

Functions (`L18 p9`–`L18 p11`): `f: X → Y`; `f  X × Y` such that for each `x  X` there is a unique `y  Y` with `(x, y)  f`. Domain `X`, **co-domain** `Y` (hyphenated in print), range `f(X) = {f(x)`

`: x  X}`. Image of a subset `f(A)`; **inverse image or preimage** `f ¹(B)` — both words are given as correct.

Diagrams

This is what the decks actually draw. Nine idioms recur; everything else is a one-off and is labelled as such.

1. Nested closed curves for containment (Euler style)

Number systems are drawn as **concentric plain closed curves with each label written inside its own region** — `: rational numbers` outermost, containing `: integers`, containing `: natural numbers`; labelled above the frame, `¯: irrational numbers` in a separate adjacent panel. Thin blue rule dividing the two panels; curves thin black; no shading; no element dots. `L05 p1`. **Seen once for number systems**, but the same nested-oval idiom recurs for subsets at `L17 p3` and `L18 p3`, so the shape convention is safe — the specific number-system figure is not.

2. Rectangle partitions

A **plain rectangle with a thin blue/teal outline** stands for the ambient set; **thin internal straight lines** split it into disjoint parts; each part is labelled in **red italic** with its superscript-qualified name; the ambient set's own label sits **above and outside** the top-left corner. Two instances on one page: split into `^even | ^odd`, and split into `^{ 1} | ^prime / ^composite`. `L07 p2`. **Seen on one page only** — but it is the course's only *printed* partition figure, and it is the natural pairing with the superscript set notation above.

3. Two-circle Venn diagrams

- **Exactly two circles of equal radius, overlapping, drawn side by side in a horizontal row**; thin black outline; labels `A` and `B` placed **inside** each circle near its top outer edge.
- **The region being denoted is filled solid grey.** The undecorated pair is drawn first, unshaded, as the reference.
- **The expression it depicts is the caption, centred directly beneath** — `(A - B)`, `(B - A)`.
- `L18 p2`. Three diagrams in a row.
- Hand-drawn variant at `L18 p3`: a **rectangle for the universe with red diagonal hatching** over the complement region, with `A` (green) inside `B` (green outline) inside it.

Critical rule, stated by the course itself: at `L18 p2` a hand annotation brackets all three Venn diagrams and writes "**not a proof!**". A Venn diagram in this course illustrates a set statement; it never discharges one. Proofs go through the element method, the laws of logical equivalence, or the set identities (`L18 p4`).

4. Small icon strip for set relations

A row of thumbnail two-set diagrams, one per notation, aligned under the list of symbols they gloss: **set A drawn as a green ellipse, set B as a pale blue/grey ellipse**; an element as a small filled dot; the operation's region filled or hatched in blue. `L17 p1` (the full strip: `x  A`, `A  B`, `A  B`, `A  B`, `A  B`, `A - B`, and `A = B` drawn as coincident ellipses). Repeated as single icons at `L17 p3`, `L17 p4`, `L17 p6`. **The green-A / grey-B colour pairing holds across all five appearances.**

5. Function arrow diagrams (bipartite)

- **Two vertical ellipses side by side: the domain `X` on the left, the co-domain `Y` on the right**, each labelled **beneath** the ellipse in blue.
- Elements are **labelled dots stacked vertically inside** each ellipse.
- Each element of `X` is joined to its image by a **straight blue line segment**. Flow is left to right.
- A subset under discussion is marked by a **translucent coloured blob** drawn around the relevant dots, labelled just outside in the matching colour with its expression (`f({2,3})`, `f ⁻¹({1})`, `f({1})`).
- `L18 p11` — four diagrams on the page, all hand-drawn, all following this arrangement.

6. Cartesian-plane graphs

Axes as **thin double-headed arrows crossing at the origin**; the `y` label at the top of the vertical axis and the `x` label at the right of the horizontal axis, both immediately beside the arrowhead; the curve in **blue**; marked points as **filled dots labelled with their coordinate pair** `(0,1)`, `(5,11)`; a **prose caption centred beneath** (`Plot of the function y = 2x + 1.`, `not a function`, `a function`). The vertical line test is shown as a **red vertical line** crossing the curve twice. `L18 p9` — three panels in a row.

7. Number lines

Drawn as a **horizontal line with an arrowhead at each end**, evenly spaced tick marks, **integer labels beneath the ticks**, and marked points or brackets **above** the line. `L11 p2` (two of them: the real line from −5 to 4 for floor/ceiling, and a minimal one showing only `k` and `k+1` with `k + ½` between); `L17 p6` (interval `[a,b]` drawn above the line with filled dots at the closed endpoints, the axis labelled at the right end).

8. Colour-coded correspondence diagrams

The single most information-dense idiom in the course. At `L06 p6`, the negation of a two-quantifier statement is shown as **two copies of the same statement schema stacked one above the other and horizontally aligned part-for-part**, with each corresponding pair of parts underlined in its own colour and joined by a **double-headed arrow of that colour**:

- red: `x  X  x  X such that`
- green: `y  Y such that  y  Y,`
- cyan: `P(x,y)  P(x,y)`
- a purple curved double-headed arrow spanning both rows, **labelled `negation`**

Seen once, but it is the canonical figure for the topic. The same alignment-plus-colour technique without arrows appears at `L03 p9` and `L12 p3`.

9. Algorithm and process cascades

- **Euclidean algorithm** (`L12 p6`): the successive equations `a = bq + r` stacked vertically down the left; each numeral wrapped in a **pastel capsule, and each number keeps the same capsule colour as it migrates** from `b` to `a` and `r` to `b` on the next line; **red diagonal arrows** trace those two migrations; a parallel right-hand column carries the matching `gcd(a,b) = gcd(b,r)` chain with the same capsule colours. Colour here is pure identity-tracking.
- **Sequence hops** (`L16 p2`, `L16 p3`, `L15 p5`): terms written in a horizontal row, **short curved arrows above or below each gap, labelled with the operation** (`+3`, `×3`, `× −1`).
- **Recursive-construction tree** (`L15 p6`): root at the **left**, branches as plain straight segments fanning **rightwards**, node labels at the branch tips, **no arrowheads on the branches**. The separate derivation chain uses arrows with the rule name written above: `--1--> 1 --1--> 11 --01--> 1101` (`L15 p7`).
- **State sequences** (`L16 p11`, Tower of Hanoi): three vertical blue pegs on a base line; discs as short red horizontal bars, widest at the bottom; **each state enclosed in a plain black rectangle**; states run **left to right**; green curved arrows between states labelled with the move count (`m_{n-1}`, `1`, `m_{n-1}`).
- **Partitions of a set as coloured blobs** (`L17 p10`): irregular non-overlapping closed curves in distinct colours, each containing dots, each **labelled just outside in its own colour** (`A` green, `A` red, `A` yellow, `A` blue). On the same page a number line is partitioned instead by **weaving highlighter stripes** — pink for `S`, green for `T` — over the tick labels.

Tables

- Full ruled grid, header row present.

- Truth tables as described above.
- Comparison tables put the item varying across the top and the cases down the side, with T/F in the cells (L06 p2: three quantified statements across, three sets S down).
- **Material reproduced from the examination formula sheet is pasted as an image and therefore appears in serif LaTeX type**, visually distinct from the sans-serif slide body: L02 p9 (Logical Equivalences), L04 p3 (Valid Argument Forms), L18 p6 (Set Identities). If reproducing one of those tables, reproduce the formula sheet's own wording and numbering.

Inconsistencies

The course does these things more than one way. **Both readings are recorded; no winner is picked. A decision is needed before any new figure fixes one.**

1. **End-of-proof mark.** Printed proofs use (L07 p3, L10 p11). Handwritten proofs use a hand-drawn square (L09 p4) *or* // (L13 p7, L18 p7). At L11 p6 the lecturer offers all of //, , and QED as equivalent. Clinch's printed induction proofs (L14 p7, L16 p6) end with a concluding sentence and **no mark at all**. Four options, all sanctioned. **Decide.**

2. **Contradiction mark.** Davies writes ( ) (L08 p3, L08 p5, L08 p6, L08 p7, L08 p8, L09 p6). Clinch writes a crossed glyph and uses it as a noun — "(proof by)" (L14 p6, two occurrences on one page). **Decide.**

3. **Name of the induction principle.** Within four decks: "by the principle of mathematical induction" (L13 p6), "by PMI" (L13 p8, L16 p12), "by MI" (L16 p10), "by SMI" (L14 p5, L16 p8), "by PSMI" (L14 p3, L14 p7). PMI/MI and SMI/PSMI are used for the same two principles in the same lecturer's decks. **Decide.**

4. **Sequence delimiters.** Printed: {b }_{n 0} (L13 p2), {a }_{n 1} (L15 p3), and bare a , a , a , … (L14 p3, L16 p2). Handwritten on the same slide (L13 p1): (a)_{n 0} **and** {a }_{n=1}^{ω}. Four forms. **Decide.**

5. **Set-builder separator.** Vertical bar in {n | n 2 (mod 8)} (L17 p3), {(x,y)|x and y } (L18 p9); colon in f = {(x,y) × : y = 2x + 1} (L18 p9, same page), f [1](B) = {x X : f(x) B} and f(A) = {f(x): x A} (L18 p11). Both on the same page as each other. **Decide.**

6. **Multiplication sign.** Printed slides use the centred dot: 1232 · 4 (L12 p6), 2 · 3 · 5 · 7 (L10 p11). Handwriting on the very next slide uses ×: 2431 × 1 (L12 p7), 4 × 9 (L13 p9), ×3 (L16 p2). **Decide.**

7. **Set difference symbol.** A − B throughout the printed slides and the formula sheet; A \ B explicitly declared equally correct at L17 p1. Not a conflict of fact, but a live choice.

8. **Which box shape carries a named principle.** Purple rounded rectangle for Theorem/Lemma/Definition/Fact (L07 p1, L10 p7, L11 p3) versus a **red** rectangle for the Well-ordering Principle (L14 p6). Same category of object, two shapes.
9. **Text colour inside the purple definition box.** Red at L07 p1, L08 p2, L11 p7; blue at L10 p7 (Unique Factorisation Theorem); black at L07 p2 (the two Facts). Three colours for the same box type.
10. **Capitalisation of the induction step labels.** "Inductive hypothesis" (L13 p6, L14 p3) versus "Inductive Hypothesis" (L16 p6, L16 p8, L16 p10). Also "Let P(n) **be** the predicate" (L13 p7, L16 p6) versus "Let P(n) **denote** the predicate" (L13 p6).
11. **LHS versus L.H.S.** L.H.S / R.H.S with stops at L13 p1; LHS / RHS without at L13 p6, L13 p7, L16 p7, L16 p9.
12. **Does contain 0?** The printed diagram at L05 p1 shows : natural numbers nested inside without saying which. The handwritten annotation on the same slide gives both = {0,1,2,…} **and** = {1,2,3,…} with the note "**take care!**" — the course is deliberately flagging the ambiguity rather than settling it. ^nonneg = {0,1,2,3,…} is defined unambiguously on the same slide and is the safe alternative.
13. **Writing two variables in the same domain.** Three forms shown side by side at L06 p5: x D and y E … (annotated "more clear"), x D and y E …, and x, y D … (annotated "short hand for same domain"). Preference is hinted at but not stated as a rule.

Not established by the source

Be candid: these are where a new diagram would be inventing, not conforming.

- **Arrowheads on function-diagram connectors.** Every mapping at L18 p11 is drawn with a **plain line segment**. Whether an arrowhead is intended, required, or merely omitted in fast handwriting cannot be told from one page. Nothing in the corpus shows an arrowheaded mapping diagram.
- **Three-set Venn diagrams.** Only two-circle Venns are ever printed (L18 p2). The set identities involving three sets (associative, distributive — L18 p6) are never illustrated. There is no evidence for the standard three-circle arrangement, region labelling, or which regions get shaded.
- **A universe rectangle in printed Venn diagrams.** L18 p2 has no enclosing rectangle at all. The only universe rectangle appears in a hand annotation (L18 p3) with red diagonal hatching. Whether a printed figure should include U is unsettled.
- **Shading colour and fill style.** One printed instance uses solid mid-grey (L18 p2); the icon strip uses blue hatching and blue solid interchangeably on the same row (L17 p1). No stated palette.

- **Line weights, stroke colours for plain geometry, and typeface.** Nothing is specified anywhere. Slide body text is a Calibri-like sans; reproduced formula-sheet extracts are serif LaTeX. Beyond that, invent nothing.
- **Figure numbering and cross-referencing.** No figure in 176 pages carries a number or the word "Figure". There is no established way to refer to a diagram from body text.
- **Any convention for the second half of the course.** L19–L36 have no decks in this set. That means **nothing is established** for: one-to-one / onto / inverse function diagrams; composition diagrams; cardinality and countability arguments (the Schröder–Bernstein theorem is on the formula sheet but never drawn); **relation digraphs**; **Hasse diagrams** for partial orders; equivalence-class pictures; Cayley tables for groups; counting trees and Pascal's triangle; **graph drawings** (vertex shape, edge style, labelling, directedness); walks/trails/circuits notation; **adjacency-matrix layout**; and tree drawings for graph theory. The only graph-theoretic images in the corpus are the Königsberg bridge photograph and a Tower of Hanoi photograph on `L01 p13`, which establish nothing.
- **Whether hand-annotation colour should be reproduced at all.** The ink layers exist because the slides are annotated live. A clean redrawn figure has no equivalent of "second colour for the second pass", and the corpus gives no printed-only version of most annotated diagrams to copy from.
- **A logic-gate or circuit notation.** None appears; MATH1061 is not a circuits course, but `L01 p10` motivates logic via computer science, so the absence is worth stating.
- **Whether may ever mean plain subset.** The course defines it as *proper* subset (`L17 p3`) and uses it that way consistently in the pages seen, but never says "we never use loosely", so a reader coming from other texts has no explicit prohibition to point at.

The Pigeonhole Principle

If more objects are put into boxes than there are boxes, some box gets two. That is the pigeonhole principle, and it proves that something **must exist** (two chosen numbers that are consecutive, two subsets with the same sum, two vertices with the same degree) without finding it. This note states the principle, gives its form for functions and its generalised form, explains how to choose the pigeons and the holes, and works through the standard arguments. Counting the pigeons and the holes uses counting-principles[140] and counting-selections[141]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[142].

The principle

> **The pigeonhole principle.** If n pigeons fly into m pigeonholes and $n > m$, then at least one pigeonhole contains two or more pigeons.

[140] courses/math1061/counting-principles.pdf
[141] courses/math1061/counting-selections.pdf
[142] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Proof. Suppose every hole contains at most one pigeon. Then the m holes contain at most m pigeons in total. But there are $n > m$ pigeons, a contradiction. So some hole contains at least two. □

Three things about it:

- **It says some hole has two, not which hole.** A pigeonhole proof is an existence proof.
- **It needs $n > m$ strictly.** Nine pigeons in nine holes can sit one per hole.
- **It says nothing when $n \leq m$.** Then two pigeons might share a hole or might not, and the principle gives no information either way.

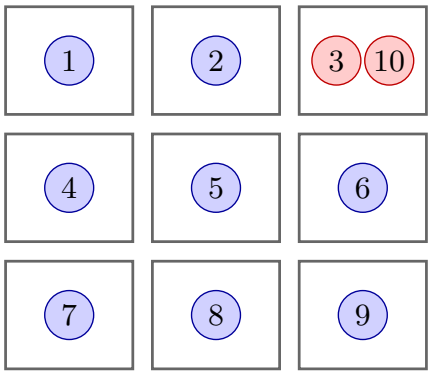


Figure 20: Ten pigeons, numbered, in nine holes. However the ten are placed, the nine holes cannot each hold at most one, since that accounts for only nine pigeons. Here pigeons 3 and 10 share the top-right hole. A different placement would make a different pair share a hole, but some hole always holds two.

As a statement about functions

Putting each pigeon in a hole is a function from the set of pigeons to the set of holes, and "two pigeons in one hole" says two inputs have the same output. So:

> **Pigeonhole principle, function form.** If X and Y are finite sets with $|X| > |Y|$, then no function $f : X \to Y$ is one-to-one: there are $x_1 \neq x_2$ in X with $f(x_1) = f(x_2)$.

This is the first of the facts about finite sets in cardinality[143], and "one-to-one" is defined in one-to-one-and-onto-functions[144]. Read this way, a pigeonhole proof has three parts: say what

[143] courses/math1061/cardinality.pdf
[144] courses/math1061/one-to-one-and-onto-functions.pdf

X is (the pigeons), say what Y is (the holes), and say what f does (which hole each pigeon goes to). Then count both sets.

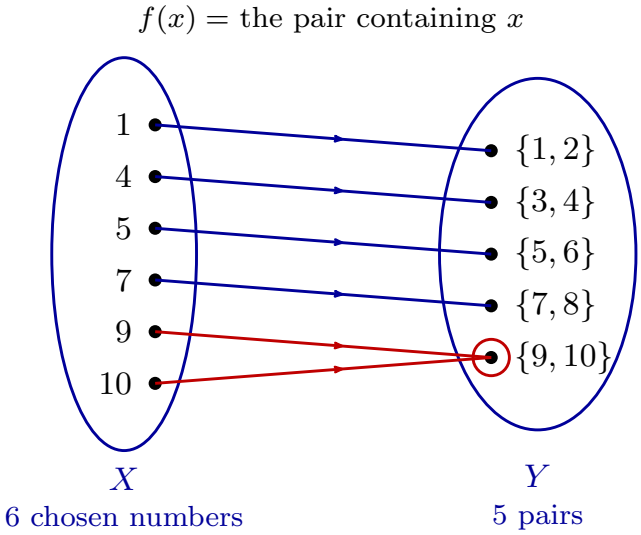


Figure 21: The function form on a small case: six numbers chosen from 1 to 10. X is the set of chosen numbers, the pigeons. Y is the set of five pairs of neighbours $1,2,3,4,\dots,9,10$, the holes. f sends each chosen number to the pair it lies in. Since $|X| = 6 > 5 = |Y|$, f cannot be one-to-one, so two chosen numbers, here 9 and 10, go to the same pair, and two numbers in one pair are consecutive. A different choice of six moves the collision to a different pair but cannot avoid one.

The generalised principle

Sometimes two in a hole is not enough, and the argument needs three, or more. The same proof gives the standard generalisation:

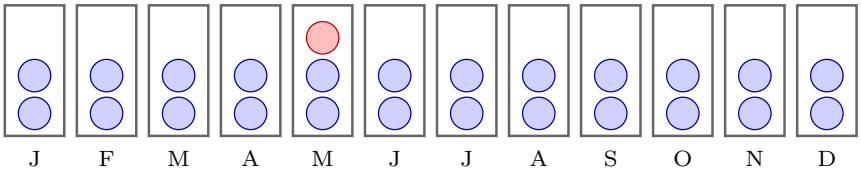
> **Generalised pigeonhole principle.** If n pigeons fly into m pigeonholes and $n > k \cdot m$, then at least one pigeonhole contains $k+1$ or more pigeons.

Proof. If every hole contained at most k pigeons, there would be at most $k \cdot m$ pigeons, and there are more. □

With $k = 1$ it is the ordinary principle. An equivalent way to say it: **some hole contains at least $\lceil n/m \rceil$ pigeons**, the average rounded up. If $n > k \cdot m$ then $n/m > k$, so $\lceil n/m \rceil \geq k+1$.

Example: birth months. Among any 25 people, at least 3 were born in the same month. The people are the pigeons and the 12 months are the holes. $25 > 2 \cdot 12$, so some month has at

least $\lceil 25/12 \rceil = 3$ of them. 24 people are not enough: two born in each month have no three in the same month.



$24 = 2 \cdot 12$ people fit two to a month; the 25th makes a month with 3

Figure 22: The generalised principle with 25 people and 12 months. Up to 24 people can be spread so that no month has more than 2, two in every month. That fills every month to its limit, so the 25th person, in red, must make some month's count 3. In general, more than $k \cdot m$ pigeons in m holes force some hole to hold $k + 1$.

Choosing the pigeons and the holes

The principle is easy. The work is in choosing what the pigeons and the holes are.

- **The pigeons** are usually the objects the problem chooses: the numbers selected, the subsets, the people, the vertices.
- **The holes** must cover everything. Every pigeon has to land in some hole, and in exactly one. When the pigeons are elements of a set, the holes are a partition of that set (sets-and-set-notation[145]).
- **Two pigeons in one hole must give exactly what is wanted.** This is what decides the holes. To force two consecutive numbers, make the holes pairs of consecutive numbers. To force a sum of 101, make the holes pairs that sum to 101. To force a common remainder, make the holes the remainders.
- **Count both.** The argument works only if there are more pigeons than holes. If the first choice of holes gives too many, look for a way to merge them, as in equal degrees, or a better bound, as in subset sums.

Many problems ask for the **largest** (or smallest) number with some property. The answer always has two halves:

1. **An example.** Show that the number can be reached, by writing down a selection of that size.
2. **A pigeonhole argument.** Show that one more forces the property to fail.

The pigeonhole half on its own proves only a bound. Without the example, the true answer might be smaller.

[145] courses/math1061/sets-and-set-notation.pdf

Worked: no two consecutive

> What is the largest number of integers that can be chosen from $\{1, 2, \dots, 100\}$ with no two consecutive?

50. The odd numbers $1, 3, \dots, 99$ are 50 numbers with no two consecutive. For the bound, the holes are the 50 pairs $\{1, 2\}, \{3, 4\}, \dots, \{99, 100\}$. Each pair is two consecutive numbers, so a good selection takes at most one from each pair. Choosing 51 or more puts two in some pair, and they are consecutive.

In general, from $\{1, 2, \dots, 2m\}$ the largest selection with no two consecutive has m numbers. The holes are pairs of neighbours, $\{2i - 1, 2i\}$.

The full question, with the wrong options, is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[146].

Worked: a pair with a given sum

> Prove that if 51 numbers are chosen from $\{1, 2, \dots, 100\}$, then two of them sum to 101.

The holes are the 50 pairs $P_i = \{i, 101 - i\}$ for $i = 1, \dots, 50$:

$$\{1, 100\},\ \{2, 99\},\ \dots,\ \{50, 51\}.$$

Each number from 1 to 100 is in exactly one of them. 51 chosen numbers in 50 pairs put two in one pair P_i, and $i + (101 - i) = 101$.

The same holes answer any question of this shape. From $\{1, 2, \dots, 2m\}$, any $m + 1$ numbers include two that sum to $2m + 1$, using the pairs $\{i, 2m + 1 - i\}$. And m numbers are not enough: $1, 2, \dots, m$ have no two summing to more than $2m - 1$.

The drawing of these pairs is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[147].

[146] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[147] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Worked: no three consecutive

> What is the largest number of integers that can be chosen from $\{1, 2, \dots, 60\}$ with no three consecutive?

40.

- **Example.** Choose everything except the multiples of 3, the numbers congruent to 1 or 2 mod 3. Any three consecutive integers include a multiple of 3, so no three chosen numbers are consecutive. That is $60 \cdot \frac{2}{3} = 40$ numbers.
- **Bound.** The holes are the 20 blocks $\{1, 2, 3\}, \{4, 5, 6\}, \dots, \{58, 59, 60\}$. A block with all three chosen is three consecutive numbers. With 41 numbers in 20 blocks, $41 > 2 \cdot 20$, so by the generalised principle some block holds $\lceil 41/20 \rceil = 3$ chosen numbers.

This is the generalised principle with $k = 2$: the property needs three in one hole, not two.

Worked: two subsets with the same sum

> Show that if A is any 6-element subset of $\{1, 2, \dots, 12\}$, then A has distinct subsets X and Y with the same sum.

- **Pigeons: the subsets of A.** There are $2^6 = 64$ of them, including $\emptyset$ and A (sets-and-set-notation[148], binomial-coefficients[149]).
- **Holes: the possible sums.** Every element is positive, so a subset's sum is between 0 (for $\emptyset$) and the sum of all of A. Six different integers from 1 to 12 add up to at most $7 + 8 + 9 + 10 + 11 + 12 = 57$. So there are at most 58 possible sums, $0, 1, \dots, 57$.
- **Conclusion.** $64 > 58$, so two different subsets have the same sum.

The pigeons here are not the elements of A but its subsets, which are far more numerous than the possible sums: the number of subsets doubles with each extra element, while the largest possible sum grows by at most 12. That gap is what makes the argument work. The bound on the sum has to be the tight one. Using the sum of all of $\{1, \dots, 12\}$, 78, as the bound gives 79 holes for 64 pigeons, and the argument fails.

Leaving out $\emptyset$ works too: 63 non-empty subsets and 57 possible sums, $1, \dots, 57$. Either way, count the pigeons and the holes over the same collection.

The figure for $A = \{2, 4, 6, 8, 10, 12\}$ is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[150].

[148] courses/math1061/sets-and-set-notation.pdf
[149] courses/math1061/binomial-coefficients.pdf
[150] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Worked: two with the same remainder

> Show that among any $n+1$ integers there are two whose difference is divisible by n.

The holes are the n possible remainders on division by n, $0, 1, \dots, n-1$. Each integer has exactly one, by the quotient-remainder theorem (modular-arithmetic[151]). $n+1$ integers and n remainders put two integers a and b in one hole. They have the same remainder r, so $a = nq_1 + r$ and $b = nq_2 + r$, and $a - b = n(q_1 - q_2)$ is divisible by n.

n integers are not enough: $0, 1, \dots, n-1$ have all their differences between $-(n-1)$ and $n-1$, and none of those but 0 is divisible by n.

For example, among any 4 integers, two differ by a multiple of 3. From $\{1, 2, \dots, 100\}$ that means 4 picks guarantee such a pair, while the 3 picks $1, 2, 3$ do not.

Worked: two vertices of equal degree

> Show that in any simple graph with at least two vertices, two vertices have the same degree.

Graphs, simple graphs and degree are in [graphs]. Said with people: in any group of two or more people, two of them have the same number of friends within the group, if friendship goes both ways.

Let the graph have $n \geq 2$ vertices. In a simple graph a vertex is joined to at most each of the other $n-1$ vertices once, so every degree is one of the n values $0, 1, \dots, n-1$. That is n pigeons and n holes, which is not enough. The extra step is that **0 and $n-1$ cannot both occur**. A vertex of degree $n-1$ is joined to every other vertex, so no vertex has degree 0. So the degrees all lie in $\{0, 1, \dots, n-2\}$ or all lie in $\{1, 2, \dots, n-1\}$. Either way there are only $n-1$ holes for n vertices, and two vertices share a degree.

This is the problem about five friends in 2026-07-27-welcome-and-intro-problems[152].

Common mistakes

- **Using it with too few pigeons.** If the number of pigeons is not more than the number of holes, the principle proves nothing. It does not make the statement false either: every 5-element subset of $\{1, \dots, 12\}$ also has two subsets with equal sums, but with 32 subsets and up to 51 possible sums the pigeonhole argument cannot show it.
- **Holes that overlap.** Pairs like $\{1, 2\}, \{2, 3\}, \{3, 4\}, \dots$ share numbers, so a pigeon is in two holes and the count no longer works. The holes must split the set: every pigeon in exactly one hole.

[151] courses/math1061/modular-arithmetic.pdf
[152] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

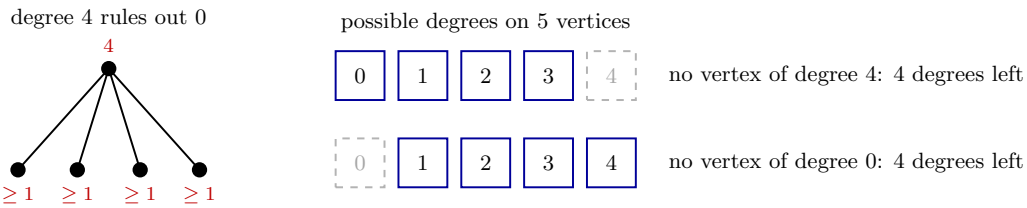


Figure 23: Why two vertices of a simple graph on 5 vertices have equal degree. The possible degrees are 0 to 4, five holes for five vertices, which forces nothing. But a vertex of degree 4 is joined to all four others, left, so each of them has degree at least 1 and none can have degree 0. So either no vertex has degree 4, top right, or none has degree 0, bottom right. In both cases only four degrees are available for five vertices, and two vertices share one.

- **Holes that don't force the property.** Two pigeons in one hole must give what is wanted. Pairs $\{1,2\},\{3,4\},\ldots$ force two consecutive numbers but not two that sum to 101.
- **Only half an answer.** For "what is the largest", the pigeonhole bound needs an example of that size as well, and the example needs the bound.
- **Off by one in the generalised form.** $k \cdot m$ pigeons can sit k to a hole. It takes $k \cdot m + 1$ to force $k + 1$ in one hole: 24 people can have no three sharing a birth month, 25 cannot.
- **A loose bound on the holes.** Counting more holes than can actually be used (sums up to 78 rather than 57, or degrees 0 to $n - 1$ when 0 and $n - 1$ exclude each other) can make an argument that should work fail.
- **Claiming to know which hole.** The principle says some hole has two pigeons. It does not say which.

See also

- cardinality[153] — no one-to-one function from a larger finite set to a smaller one, which is the principle for functions
- one-to-one-and-onto-functions[154] — what one-to-one means
- [graphs] — degree, used in equal degrees
- counting-selections[155] — counting the pigeons and the holes
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[156] — Lecture 33

[153] courses/math1061/cardinality.pdf
[154] courses/math1061/one-to-one-and-onto-functions.pdf
[155] courses/math1061/counting-selections.pdf
[156] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

- 2026-10-26-walks-trails-and-circuits[157] — Lecture 34, which opens with equal degrees again
- practice-problems[158] — §42, with full worked solutions

Practice Problems — the Semester-wide Set

This is the course's one problem set for the whole semester — a single document rather than a per-week handout. 46 sections, one per pre-work video, each with the relevant textbook pages, a set of practice problems and full worked solutions. Everything is reproduced here in full, so you never need to open the PDF.

Applied Classes start in **Week 2** and run to Week 13 — twelve of them, matching the "best 8 of 12" Applied Classes component worth 30% (see math1061[159]). Each week's class applies the *previous* week's lecture content, so the material a class covers runs roughly one week behind the lecture column below. Which sections a given Applied Class draws on is not stated in any of the source material.

These problems belong to the roughly three hours of individual study each week, which are for revising the videos, readings and classes **and completing the Practice Problems**. They are the out-of-class half of the course, and they are *not* the same thing as the Assessed Exercises, which are done and submitted inside the class itself. (That class goes by two names, the **Active Class** and the **Applied Class**. They are one session.)

How each section is laid out

1. Relevant textbook pages for Epp 4th edition and 5th (metric) edition
2. **Practice problems**
3. **Solutions** — full worked solutions, not just answers
4. Occasionally a non-assessable **Application** block (see the table below)

Errata

The source document carries an errata page listing corrections made during semester. **Last update: 24 August 2026**, with two entries:

- On page 195, the solution to 1(b) was corrected (the note in brackets had previously copied the note from 1(a)) — already applied in §45 below.
- **Question 2 in section 30 has been updated, and the original version moved to section 32** (because it refers to antisymmetry) — applied in §30 and §32 below.

[157] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[158] courses/math1061/practice-problems.pdf
[159] courses/math1061/math1061.pdf

If something looks wrong, post on the Ed Discussion board.

Section index

Every section is below, with its topic and textbook page ranges. Each section goes with one pre-work video (§1 with *Video 001*, and so on up to *Video 046*), and the Lecture (week) column places it in the schedule of math1061[160] by that video number. The Notes column links to the concept note covering that material where one exists; the rest are still ahead in the semester.

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
1	Logical Form	L2 (wk 1)	023–029	037–043	logical-connectives[161]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[162]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[163]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[164]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[165]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[166]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[167]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[168]

[160] courses/math1061/math1061.pdf
[161] courses/math1061/logical-connectives.pdf
[162] courses/math1061/logical-equivalence-laws.pdf
[163] courses/math1061/conditional-statements.pdf
[164] courses/math1061/valid-argument-forms.pdf
[165] courses/math1061/determining-argument-validity.pdf
[166] courses/math1061/quantified-statements.pdf
[167] courses/math1061/quantified-statements.pdf
[168] courses/math1061/quantified-statements.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[169]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[170]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[171]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[172]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[173]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[174]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[175]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[176]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[177]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[178]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[179]

[169] courses/math1061/proof-techniques.pdf
[170] courses/math1061/proof-techniques.pdf
[171] courses/math1061/proof-techniques.pdf
[172] courses/math1061/rational-and-irrational-numbers.pdf
[173] courses/math1061/divisibility-and-factorisation.pdf
[174] courses/math1061/modular-arithmetic.pdf
[175] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[176] courses/math1061/sequences-and-summations.pdf
[177] courses/math1061/mathematical-induction.pdf
[178] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[179] courses/math1061/recursive-definitions.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[180]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[181]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[182]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[183]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[184]
25	one-to-one, Onto, and Inverse Functions	L19 (wk 7)	397–416	439–461	
26	Composition of Functions	L20 (wk 7)	416–427	461–472	
27	Cardinalities	L21 (wk 8)	428–441	473–486	
28	Countable and Uncountable Sets	L22 (wk 8)	428–441	473–486	
29	Relations on Sets	L23 (wk 8)	442–449	487–494	
30	Reflexivity, Symmetry, Transitivity	L23 (wk 8)	449–459	495–505	
31	Equivalence Relations	L24 (wk 9)	459–478	505–523	
32	Partial Order Relations	L25 (wk 9)	498–515	546–563	

[180] courses/math1061/solving-recurrence-relations.pdf
[181] courses/math1061/sets-and-set-notation.pdf
[182] courses/math1061/sets-and-set-notation.pdf
[183] courses/math1061/proving-set-properties.pdf
[184] courses/math1061/functions-on-general-sets.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
33	Definitions and Examples of Groups	L26 (wk 9)	—	—	
34	Elementary Properties of Groups	L27 (wk 10)	—	—	
35	Group Isomorphisms	*not scheduled*	—	—	
36	Definitions and Examples of Fields	L28 (wk 10)	—	—	
37	Introduction to Counting	L29 (wk 11)	516–553	564–604	
38	Counting Selections	L30 (wk 11)	516–553	564–604	
39	Introduction to Probability	L31 (wk 12)	516–553	564–604	
40	Binomial Coefficients	L31 (wk 12)	565–591	617–641	
41	Inclusion Exclusion	L32 (wk 12)	545–549	595–599	
42	The Pigeonhole Principle	L33 (wk 12)	554–565	604–616	
43	Introduction to Graph Theory	L33 (wk 12)	625–660	677–697	
44	Walks, Trails and Circuits	L34 (wk 12)	625–660	677–697	
45	Matrix Representations of Graphs	L35 (wk 13)	661–675	698–712	
46	Trees	L36 (wk 13)	683–701	720–742	

§35 Group Isomorphisms has no lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36). The section itself carries no practice problems and is

marked *optional and will not be assessed*, so the gap is deliberate.

§28 Countable and Uncountable Sets carries its own note in the source: *this content will not be assessed in MATH1061.* It still has a full set of problems and solutions.

Sections 33–36 (groups and fields) list no textbook page ranges.

Non-assessable application blocks

Eight sections carry an extra block of problems, **not assessable for MATH1061**, mostly drawn from K. Rosen, *Discrete Mathematics and its Applications*, 7th ed. (1991), with two from Epp. They connect the pure material to computer science, and are reproduced in full alongside their sections.

After §	Block	Source
2	Applications to Computer Science — bit strings and logic circuits	Rosen pp. 20–24
5	Applications of Valid and Invalid Arguments	Rosen pp. 48–68
9	Applications of Proofs to Computer Science — resolution and automated theorem proving	Rosen pp. 74–80
15	Trace Tables for Algorithms — the Division and Euclidean algorithms	Epp §4.8 (4th ed.) / §4.10 (5th ed.)
21	Computer Representations of Sets	Rosen pp. 134–138
28	Computability of Functions	Rosen pp. 170–177
31	Identifiers — C identifiers as an equivalence-relation example	Rosen pp. 608–618
37	Runtime — counting basic instructions	Epp 5th ed. pp. 787–799

A note on the diagrams: the source PDF draws logic circuits, graphs and Hasse diagrams as figures. Those are reproduced here as explicit gate netlists and edge lists, which carry the same information in a form that renders everywhere.

§1 — Logical Form

Epp 4th ed. pp. 023–029 · 5th ed. (metric) pp. 037–043. Lecture 2 (week 1). Notes: logical-connectives[185].

Problems

1. Write a truth table for the statement form $p \wedge (\sim q \vee r)$.
2. Suppose you know that $(\sim p \wedge q) \vee p$ is false. What can you conclude about the truth values of each of the two variables?
3. Let p be the statement "DATAENDFLAG is off," q the statement "ERROR equals 0," and r the statement "SUM is less than 1,000." Express the following sentences in symbolic notation.
   (a) DATAENDFLAG is off, ERROR equals 0, and SUM is less than 1,000.
   (b) DATAENDFLAG is off but ERROR is not equal to 0.
   (c) DATAENDFLAG is off; however, ERROR is not 0 or SUM is greater than or equal to 1,000.
   (d) DATAENDFLAG is on and ERROR equals 0 but SUM is greater than or equal to 1,000.
   (e) Either DATAENDFLAG is on or it is the case that both ERROR equals 0 and SUM is less than 1,000.

Solutions

1. The truth table is

p	q	r	$\sim q$	$\sim q \vee r$	$p \wedge (\sim q \vee r)$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	T	T	F
F	F	F	T	T	F

[185] courses/math1061/logical-connectives.pdf

2. We know $(\sim p \wedge q) \vee p$ is false. A disjunction is false only when both parts are false, so we must have

$$p \text{ is false} \quad \text{and} \quad (\sim p \wedge q) \text{ is false.}$$

From p being false, it follows that $\sim p$ is true. Now $(\sim p \wedge q)$ can be false only if q is false (since $\sim p$ is already true). Hence q is false.

Therefore p **is false and** q **is false**.

3. (a) $p \wedge q \wedge r$.

(b) $p \wedge \sim q$.

(c) $p \wedge (\sim q \vee \sim r)$.

(d) $\sim p \wedge q \wedge \sim r$.

(e) $\sim p \vee (q \wedge r)$.

§2 — Logical Equivalence

Epp 4th ed. pp. 030–038 · 5th ed. (metric) pp. 043–053. Lecture 2 (week 1). Notes: logical-equivalence-laws[186].

Problems

1. (a) Use the laws of logical equivalence to show that $p \wedge q \equiv \sim (\sim p \vee \sim q)$.

(b) Use the laws of logical equivalence to show that $\sim (p \vee \sim q) \vee (\sim p \wedge \sim q) \equiv \sim p$.

2. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

(a) $((p \wedge q) \vee (q \wedge r)) \vee \sim q$

(b) $(\sim p \vee q) \vee (p \wedge \sim q)$

3. Use De Morgan's laws to write sentences equivalent to the following:

(a) It is not true that I am studying Computer Science and I am studying Engineering.

(b) I am not going to the movies this weekend or I am not going swimming this weekend.

[186] courses/math1061/logical-equivalence-laws.pdf

4. Let $\oplus$ denote **exclusive or**, which means '… or … but not both'. The truth table for $p \oplus q$ is as follows:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

   (a) Use a truth table to show that $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

   (b) Use a truth table to show that $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

   (c) Use the laws of logical equivalence and the equivalence $p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$ (which is the definition of $\oplus$) to show that

$$(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r).$$

Solutions

1. (a) We have

$$\begin{aligned} \sim (\sim p \vee \sim q) &\equiv \sim (\sim p) \wedge \sim (\sim q) && \text{by De Morgan's law} \\ &\equiv p \wedge q && \text{by the double negative law (used twice).} \end{aligned}$$

   (b) We have

$$\begin{aligned} \sim (p \vee \sim q) \vee (\sim p \wedge \sim q) &\equiv (\sim p \wedge \sim\sim q) \vee (\sim p \wedge \sim q) && \text{by De Morgan's law} \\ &\equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q) && \text{by the double negative law} \\ &\equiv \sim p \wedge (q \vee \sim q) && \text{by the distributive law} \\ &\equiv \sim p \wedge \mathbf{t} && \text{by the negation law} \\ &\equiv \sim p && \text{by the identity law.} \end{aligned}$$

2. (a) We have

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \vee (q \wedge r)$	$\sim q$	$((p \wedge q) \vee (q \wedge r)) \vee \sim q$
T	T	T	T	T	T	F	T
T	T	F	T	F	T	F	T
T	F	T	F	F	F	T	T
T	F	F	F	F	F	T	T
F	T	T	F	T	T	F	T
F	T	F	F	F	F	F	F
F	F	T	F	F	F	T	T
F	F	F	F	F	F	T	T

Thus the statement is **neither a tautology nor a contradiction**.

(b) We have

p	q	$\sim p$	$\sim p \vee q$	$\sim q$	$p \wedge \sim q$	$(\sim p \vee q) \vee (p \wedge \sim q)$
T	T	F	T	F	F	T
T	F	F	F	T	T	T
F	T	T	T	F	F	T
F	F	T	T	T	F	T

Hence the statement is a **tautology**.

3. (a) Let C be the statement "I am studying Computer Science" and E be the statement "I am studying Engineering." The given statement is $\sim (C \wedge E)$. By De Morgan's law,

$$\sim (C \wedge E) \equiv (\sim C) \vee (\sim E).$$

So an equivalent statement is: "I am not studying Computer Science or I am not studying Engineering."

(b) Let M be the statement "I am going to the movies this weekend" and S be the statement "I am going swimming this weekend." The given sentence is $(\sim M) \vee (\sim S)$. By De Morgan's law (in reverse),

$$(\sim M) \vee (\sim S) \equiv \sim (M \wedge S).$$

So an equivalent statement is: "It is not the case that I am both going to the movies this weekend and going swimming this weekend."

4. (a) We have

p	q	$p \vee q$	$\sim p$	$(p \vee q) \wedge \sim p$	$q \wedge \sim p$
T	T	T	F	F	F
T	F	T	F	F	F
F	T	T	T	T	T
F	F	F	T	F	F

Since the last two columns agree on every row, we have $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

(b) We have

p	q	r	$p \oplus q$	$(p \oplus q) \wedge r$	$p \wedge r$	$q \wedge r$	$(p \wedge r) \oplus (q \wedge r)$
T	T	T	F	F	T	T	F
T	T	F	F	F	F	F	F
T	F	T	T	T	T	F	T
T	F	F	T	F	F	F	F
F	T	T	T	T	F	T	T
F	T	F	T	F	F	F	F
F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F

The columns for $(p \oplus q) \wedge r$ and $(p \wedge r) \oplus (q \wedge r)$ match on all rows, hence $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

(c) To save space, multiple laws have been applied in some steps. There are many different ways to apply the laws to prove this, so your proof may look different to this one. We have

$(p \wedge r) \oplus (q \wedge r)$

$\equiv ((p \wedge r) \vee (q \wedge r)) \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by the given equivalence (def of $\oplus$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by distributive and commutative laws (for $\wedge r$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge (r \wedge r))$	by associative and commutative laws (for $\wedge$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge r)$	by idempotent law
$\equiv (p \vee q) \wedge r \wedge (\sim (p \wedge q) \vee \sim r)$	by De Morgan's law
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee (r \wedge \sim r) \Big)$	by distributive law (for $r \wedge$)
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee \mathbf{c} \Big)$	by negation law
$\equiv (p \vee q) \wedge r \wedge \sim (p \wedge q)$	by identity law
$\equiv (p \vee q) \wedge \sim (p \wedge q) \wedge r$	by associative and commutative laws (for $\wedge$)
$\equiv (p \oplus q) \wedge r$	by the given equivalence (def of $\oplus$)

Application — Applications to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 20–24.*

Information is often represented using binary or **bit strings**, which are sequences consisting of zeros and ones. The **length** of a string is the total number of bits in it — for example 0110110 is a string of length 7. The logical operators $\wedge$, $\vee$ and $\oplus$ extend to binary strings. The operators AND, OR and XOR are:

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Propositional logic also applies to the design of computer hardware. A **digital logic circuit** receives input signals (either 0, the wire being off, or 1, on) and produces output signals which are also bits. Complicated digital logic circuits can be constructed from three basic gates: the **OR gate**, the **NOT gate** and the **AND gate**.

A **combinational circuit** uses these gates and obeys the following rules.

1. Two input wires cannot be combined without a gate.
2. A single input wire can be split partway and directed into two separate gates.
3. An output wire from a gate can be used as input for another gate.

4. No output wire from a gate can eventually feed back into that gate.

For example, the logical expression $(p \wedge \sim q) \vee \sim r$ has the combinational circuit

- NOT$(q) \to n_1$
- AND$(p, n_1) \to a_1$
- NOT$(r) \to n_2$
- OR$(a_1, n_2) \to$ output $(p \wedge \sim q) \vee \sim r$

Application problems

1. Find the bitwise OR, bitwise AND and bitwise XOR of each of these pairs of binary strings.

   (a) 1011110, 0100001

   (b) 11110000, 10101010

2. Construct a combinational circuit using the NOT, OR and AND gates that produces the outputs:

   (a) $(\sim p \vee \sim r) \wedge q$

   (b) $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. Find the output of the following combinational circuit, simplify the expression using logical laws and construct a new circuit for the simplified expression. The circuit is

   - NOT$(p) \to n_1$
   - NOT$(q) \to n_2$
   - OR$(p, n_2) \to o_1$
   - OR$(n_1, n_2) \to o_2$
   - AND$(o_1, o_2) \to a_1$
   - OR$(a_1, r) \to$ output

   (both p and q have their wires split, feeding two gates each).

4. The logical binary operation NAND, denoted $|$, is defined by

$$p \mid q \equiv \sim (p \wedge q).$$

   (a) Write down the truth table for $\sim (p \mid q)$. Show all working.

   (b) Prove, using truth tables or otherwise, that $(p \mid p) \equiv (\sim p)$. Show all working.

   (c) Prove, using truth tables or otherwise, that $((p \mid p) \mid (q \mid q)) \equiv p \vee q$. Show all working.

Application solutions

1. (a)
$$1011110 \text{ OR } 0100001 = 1111111,$$
$$1011110 \text{ AND } 0100001 = 0000000,$$
$$1011110 \text{ XOR } 0100001 = 1111111.$$

   (b)
$$11110000 \text{ OR } 10101010 = 11111010,$$
$$11110000 \text{ AND } 10101010 = 10100000,$$
$$11110000 \text{ XOR } 10101010 = 01011010.$$

2. (a) The circuit is
   - NOT$(p) \to n_1$
   - NOT$(r) \to n_2$
   - OR$(n_1, n_2) \to o_1$
   - AND$(o_1, q) \to$ output $(\sim p \vee \sim r) \wedge q$

   (b) The circuit is
   - NOT$(r) \to n_1$
   - AND$(p, n_1) \to a_1$
   - NOT$(q) \to n_2$
   - AND$(n_2, r) \to a_2$
   - OR$(a_1, a_2) \to$ output $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. The given digital logic circuit has output $((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r$. Using laws of logical equivalence we have

$$\begin{aligned}((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r &\equiv (\sim q \vee (p \wedge \sim p)) \vee r && \text{by distributive and commutative laws}\\ &\equiv (\sim q \vee \mathbf{c}) \vee r && \text{by negation law}\\ &\equiv \sim q \vee r && \text{by identity law}\end{aligned}$$

   The simplification is $\sim q \vee r$. The simplified logic circuit is
   - NOT$(q) \to n_1$
   - OR$(r, n_1) \to$ output $\sim q \vee r$

4. (a) We have

p	q	$p \wedge q$	$p \mid q$	$\sim (p \mid q)$
T	T	T	F	T
T	F	F	T	F
F	T	F	T	F
F	F	F	T	F

Hence $\sim (p \mid q)$ has the same truth values as $p \wedge q$ (it is true exactly when both p and q are true).

(b) Since $p \mid p \equiv \sim (p \wedge p)$, we have

$$p \mid p \equiv \sim (p \wedge p) \equiv \sim p$$

because $p \wedge p \equiv p$ (idempotent law). Alternatively, by truth table:

p	$p \wedge p$	$p \mid p$	$\sim p$
T	T	F	F
F	F	T	T

The last two columns agree, so $p \mid p \equiv \sim p$.

(c) First note from part (b) that $p \mid p \equiv \sim p$ and $q \mid q \equiv \sim q$. Therefore

$$\begin{aligned} (p \mid p) \mid (q \mid q) &\equiv (\sim p) \mid (\sim q) && \text{by part (b)} \\ &\equiv \sim ((\sim p) \wedge (\sim q)) && \text{by def of NAND} \\ &\equiv p \vee q && \text{by De Morgan's law.} \end{aligned}$$

Alternatively, by truth table:

p	q	$p \mid p$	$q \mid q$	$(p \mid p) \mid (q \mid q)$	$p \vee q$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	F	F

The last two columns match, hence $(p \mid p) \mid (q \mid q) \equiv p \vee q$.

§3 — Conditional Statements

Epp 4th ed. pp. 039–050 · 5th ed. (metric) pp. 053–066. Lecture 3 (week 1). Notes: conditional-statements[187].

Problems

1. Let p, q and r be statements. Use the laws of logical equivalence to show that

$$p \to (q \vee r) \equiv (p \wedge \sim q) \to r.$$

2. Let p and q be statement variables. Are the following statements logically equivalent? Justify your answer.

   - **Statement A:** $(p \to q) \wedge \sim q$
   - **Statement B:** $\sim (p \wedge q)$

3. Write each of the following statements in the form 'if … then …'.

   (a) A sufficient condition for the warranty to be good is that you bought the computer less than a year ago.

   (b) Jane gets seasick whenever she is on a boat.

4. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

   (a) $(\sim p \wedge (p \to q)) \to \sim q$

   (b) $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$

5. Negate the following two statements.

   (a) If it rains, then Sue takes her umbrella.

   (b) The cakes burn if the oven temperature is too high.

6. Recall "a sufficient condition for s is r" means r is a sufficient condition for s, and that "a necessary condition for s is r" means r is a necessary condition for s. Rewrite the following statements in 'if … then …' form:

   (a) A sufficient condition for John's team to win the championship is that it wins the rest of its games.

   (b) A necessary condition for this computer program to be correct is that it not produce error messages during translation.

[187] courses/math1061/conditional-statements.pdf

Solutions

1. We have

$$\begin{aligned} p \to (q \vee r) &\equiv \sim p \vee (q \vee r) && \text{by definition of implication} \\ &\equiv (\sim p \vee q) \vee r && \text{by the associative law} \\ &\equiv \sim (p \wedge \sim q) \vee r && \text{by De Morgan's law and double negative law} \\ &\equiv (p \wedge \sim q) \to r && \text{by definition of implication.} \end{aligned}$$

2. Let A be the statement $(p \to q) \wedge \sim q$ and let B be the statement $\sim (p \wedge q)$. Then

$$\begin{aligned} A &\equiv (\sim p \vee q) \wedge \sim q && \text{by definition of implication} \\ &\equiv (\sim p \wedge \sim q) \vee (q \wedge \sim q) && \text{by distributive and commutative laws} \\ &\equiv (\sim p \wedge \sim q) \vee \mathbf{c} && \text{by negation law} \\ &\equiv \sim p \wedge \sim q && \text{by identity law,} \end{aligned}$$

   while

$$B \equiv \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \text{by De Morgan's law.}$$

   Thus Statement A and Statement B are **not** logically equivalent because, for example, if p is false and q is true, then A is false and B is true. Hence $A \not\equiv B$.

3. (a) If you bought the computer less than a year ago, then the warranty is good.

   (b) If Jane is on a boat, then Jane gets seasick.

4. (a) **Solution Option 1.** The truth table for the statement is

p	q	$\sim p$	$p \to q$	$\sim p \wedge (p \to q)$	$\sim q$	$(\sim p \wedge (p \to q)) \to \sim q$
T	T	F	T	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

   The statement is **neither a tautology nor a contradiction**.

   Solution Option 2. The same truth table, written under the parts of the statement:

p	q	$\sim p$	$\wedge$	$(p \to q)$	$\to$	$\sim q$
T	T	F	F	T	T	F
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T
order						

The small numbers show the order in which the columns were completed. Column comes from comparing columns and . Column comes from comparing columns and , and shows the truth values for the entire statement. This shows that this statement is neither a tautology nor a contradiction. (You don't have to number the columns — this is just to help your understanding!)

(b) **Solution Option 1.** The truth tables for the LHS and RHS are:

p	q	r	$q \vee r$	$p \to (q \vee r)$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \to r$
T	T	T	T	T	F	F	T
T	T	F	T	T	F	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	F	F	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	F	T
F	F	F	F	T	T	F	T

Therefore the truth table for the statement is:

p	q	r	$(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

The statement is a **tautology**.

Solution Option 2. Another way to represent the truth table for $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$:

p	q	r	$p \to$	$(q \vee r)$	$\leftrightarrow$	$(p \wedge \sim q)$	$\to r$
T	T	T	T	T	T	F	T
T	T	F	T	T	T	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	T	F	T
F	T	F	T	T	T	F	T
F	F	T	T	T	T	F	T
F	F	F	T	F	T	F	T
order							

Here column comes from comparing columns and . We see (from column) that this is a tautology.

5. (a) Let R be the statement "it rains" and U be the statement "Sue takes her umbrella." The given statement is $R \to U$. Its negation is

$$R \wedge \sim U,$$

i.e. "It rains and Sue does not take her umbrella."

(b) Let H be the statement "the oven temperature is too high" and B be the statement "the cakes burn." The given statement is $H \to B$. Its negation is

$$H \wedge \sim B,$$

i.e. "The oven temperature is too high and the cakes do not burn."

6. (a) If John's team wins the rest of its games, then John's team will win the championship.

(b) If this computer program is correct, then it does not produce error messages during translation.

§4 — Valid and Invalid Arguments

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 4 (week 2). Notes: valid-argument-forms[188].

[188] courses/math1061/valid-argument-forms.pdf

Problems

1. State truth values for the statement variables p and q that demonstrate that the following argument is invalid, and justify your answer.

   Premise 1: q Premise 2: $p \to q$ Conclusion: p

2. Find values of the statement variables a, b and c that show that the following argument is invalid.

   1. $a \to b$
   2. $\sim a \to c$
   3. $\sim b \to c \therefore b$

3. Use a truth table to show that the following argument forms are valid.

   (a) **Elimination:**

   1. $p \vee q$
   2. $\sim q \therefore p$

   (b) **Generalisation:**

   1. $p \therefore p \vee q$

4. Use a truth table to show that the following argument is invalid.

   1. $(p \wedge q) \to \sim r$
   2. $p \vee \sim q$
   3. $\sim q \to p \therefore \sim r$

Solutions

1. To show the argument is invalid, we must find truth values for p and q such that the premises are true and the conclusion is false.

   Suppose p is false and q is true. Then Premise 1 (q) is true and Premise 2 ($p \to q$) is true (by definition of implication). However, the conclusion (p) is false. Therefore the argument is invalid.

2. To show the argument is invalid, we must find truth values for a, b and c such that the premises are true and the conclusion is false.

   Let a be false, b be false, and c be true. By definition of implication, all three premises are true, but the conclusion (b) is false, so the argument is invalid.

3. (a)

p	q	premise 1: $p \vee q$	premise 2: $\sim q$	conclusion: p
T	T	T	F	T
T	F	T	T	T
F	T	T	F	F
F	F	F	T	F

There is only one row of the truth table in which all premises are true (the second row), and here the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

(b)

p	q	premise 1: p	conclusion: $p \vee q$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	F	F

There are two rows for which all premises (here just the one premise) are true — the first two rows — and for each of these rows the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

4. We compute the truth table:

p	q	r	$(p \wedge q) \rightarrow \sim r$	$p \vee \sim q$	$\sim q \rightarrow p$	Prem. 1 $\wedge$ Prem. 2 $\wedge$ Prem. 3	$\sim r$
T	T	T	F	T	T	F	F
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	F
T	F	F	T	T	T	T	T
F	T	T	T	F	T	F	F
F	T	F	T	F	T	F	T
F	F	T	T	T	F	F	F
F	F	F	T	T	F	F	T

There are three rows for which all the premises are true, however for one of these rows the conclusion is false. In particular, taking p to be true, q to be false, and r to be true makes all the premises true but the conclusion false, so the argument is **invalid**.

§5 — Methods for Determining Validity

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 5 (week 2). Notes: determining-argument-validity[189].

Problems

1. Determine whether the following arguments are valid. If the argument is valid, prove it using rules of inference. If the argument is invalid, demonstrate it with a choice of truth values for the variables.

   (a)

   $p \to q \; q \to p \therefore p \vee q$

   (b)

   $p \; p \to q \sim q \vee r \therefore r$

   (c)

   $p \vee q \; p \to\sim q \; p \to r \therefore r$

2. Write the following argument in symbolic form. Then determine whether the argument is valid or not.

   > An error message is received if the output is flagged. The system is running normally only if the output is not flagged. An error message is received. Therefore, the system is not running normally.

   Please use the following variables:

p	the output is flagged
q	an error message is received
r	the system is running normally

[189] courses/math1061/determining-argument-validity.pdf

3. Give truth values for the variables p, q, r, s and w which demonstrate that the following argument is invalid.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

Solutions

1. (a) The argument is **invalid**. When p and q are both false, all the premises are true, but the conclusion is false. One could arrive at this example by computing the following truth table:

p	q	$p \to q$	$q \to p$	$p \vee q$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

(In the last row, the premises are true, but the conclusion is false.)

(b) The argument is **valid**, and we prove this with rules of inference:

1.	p	Premise
2.	$p \to q$	Premise
3.	$\sim q \vee r$	Premise
4.	q	from 1 and 2 by Modus Ponens
5.	r	from 3 and 4 by elimination (and the double negative law)

Therefore the argument is valid.

(c) Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is false**. Since r is false but the third premise $(p \to r)$ is true, we must have p **is false**. Since p is false, this means the second premise $(p \to \sim q)$ is also true. Now since p is false but the first premise $(p \vee q)$ is true, we must have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

2. The argument has the symbolic form:

1.	$p \to q$	(An error message is received if the output is flagged.)
2.	$r \to \sim p$	(The system is running normally only if the output is not flagged.)
3.	q	(An error message is received.)
$\therefore$	$\sim r$	(The system is not running normally.)

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is true**. Since r is true, and premise 2 is true, we must have $\sim p$ true, that is p **is false**. Since premise 3 is true, we have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

3. The argument being valid is the same as this overall implication statement being a tautology.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

We can write the argument as follows:

1. $p \vee q$
2. $q \to r$
3. $(p \wedge s) \to w$
4. $\sim r$
5. $q \to s \therefore w$

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have w **is false**. Since premise 4 is true we have r **is false**. Since premise 2 is true and r is false, we must have q **is false**. Since premise 1 is true and q is false we have p **is true**. Since premise 3 is true and w is false, we must have $(p \wedge s)$ false, and since p is true, this means s **is false**. These truth values also mean premise 5 is true.

Thus with these truth values for the variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

Application — Applications of Valid and Invalid Arguments

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 48–68.*

Application problems

1. Translating English sentences into logical expressions is an essential part of specifying both hardware and software systems. Software engineers must take requirements in English and produce precise, unambiguous specifications that can be used as the basis for system development.

   Consider the following predicates and domains:

   Predicates:

$F(x, y)$	disk x has more than y kilobytes of free space.
$S(m)$	mail message m can be saved.
$A(x)$	alert x is active.
$Q(m)$	message m is queued.
$T(m)$	message m is transmitted.
$D(s)$	the diagnostic monitor tracks the status of system s.

   Domains:

M	the nonempty set of all messages.
X	the set of all disks.
Y	the set of all alerts.
S	the set of all systems.

   Express the system specifications below using quantifiers and logical connectives:

   (a) At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.

   (b) Whenever there is an active alert, all queued messages are transmitted.

   (c) The diagnostic monitor tracks the status of all systems except the main console.

2. System specifications should be **consistent**; that is, they should not contain conflicting requirements that could be used to derive a contradiction. When specifications are not consistent, there would be no way to develop a system that satisfies all specifications. Logically, a system is consistent if it is possible for all the premises to be simultaneously true.

Use logical expressions and methods of logical deduction to determine whether the following specifications are consistent.

(a) The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode.

(b) The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed. The router does not support the new address space.

Application solutions

1. (a) $(\exists x \in X \text{ s.t. } F(x, 10)) \rightarrow (\exists m \in M \text{ s.t. } S(m))$.

   (b) $(\exists y \in Y \text{ s.t. } A(y)) \rightarrow (\forall m \in M,\ (Q(m) \rightarrow T(m)))$.

   (c) Let $c \in S$ denote the main console. $\forall s \in S,\ (s \neq c \rightarrow D(s))$.

2. (a) Define the following variables:

m	the system is in multiuser state
n	the system is operating normally
k	the kernel is functioning
i	the system is in interrupt mode

Now we can express the specifications as follows:

1. $m \leftrightarrow n$
2. $n \rightarrow k$
3. $\sim k \vee i$
4. $\sim m \rightarrow i$
5. $\sim i$

Solution Option 1. If these specifications are consistent, then we must be able to find truth values for each of the variables that makes all of the specifications true. Assume the specifications are consistent (so we assume each specification is true). For specification 5 to be true we know i **is false**. For specification 4 to be true, with i false, we know $\sim m$ is false so m **is true**. For premise 1 to be true, with m true, we have n **is true**. For specification 2 to be true, and since n is true, we have k **is true**. However, now $\sim k$ is

false and i is false, which means specification 3 is false. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

Solution Option 2. Suppose the specifications are all true. Using laws of inference, we have

1.	$m \leftrightarrow n$	specification
2.	$n \rightarrow k$	specification
3.	$\sim k \vee i$	specification
4.	$\sim m \rightarrow i$	specification
5.	$\sim i$	specification
6.	$\sim k$	from 3 and 5 by elimination (and double negative law)
7.	$\sim n$	from 2 and 6 by Modus Tollens
8.	$(m \rightarrow n) \wedge (n \rightarrow m)$	from 1 by definition of $\leftrightarrow$
9.	$m \rightarrow n$	from 8 by specialisation
10.	$\sim m$	from 9 and 7 by Modus Tollens
11.	i	from 4 and 10 by Modus Ponens

But now we have both i and $\sim i$ being true, which is a contradiction. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

(b) Define the following variables:

r	the router can send packets to the edge system
a	the router supports the new address space
s	the latest software release is installed

Now we can express the specifications as follows:

1. $r \rightarrow a$
2. $a \rightarrow s$
3. $s \rightarrow r$
4. $\sim a$

Assume the specifications are consistent, so each specification is true. For specification 4 to be true, $\sim a$ is true, so a **is false**. For specification 1 to be true with a false we must

have r **is false**. Now, since r is false and specification 3 is true, we have s **is false**. We double-check that specification 2 is true, which it is because a is false. Thus, we have found truth values of the statement variables that make all of the specifications true, so the system **is consistent**.

§6 — Quantified Statements

Epp 4th ed. pp. 096–108 · 5th ed. (metric) pp. 108–121. Lecture 5 (week 2). Notes: quantified-statements[190].

Problems

1. Rewrite each of the following in the form "∀__, __." Here, let D be the set of all dinosaurs, and let L be the set of all logicians.
   (a) All dinosaurs are extinct.
   (b) Every real number is positive, negative, or zero.
   (c) No irrational numbers are integers.
   (d) No logicians are lazy.
   (e) The number 2,147,581,953 is not equal to the square of any integer.
   (f) The number -1 is not equal to the square of any real number.
2. Rewrite each of the following in the form "∃__ such that __." Here, let X be the set of all exercises.
   (a) Some exercises have answers.
   (b) Some real numbers are rational.
3. Determine whether the following statements are true or false. Justify your reasoning.
   (a) $\forall x \in \mathbb{R},\ x \geq \frac{1}{x}$.
   (b) $\forall a \in \mathbb{Z},\ \frac{a-1}{a} \notin \mathbb{Z}$.
   (c) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

[190] courses/math1061/quantified-statements.pdf

Solutions

1. (a) $\forall x \in D,\ x$ is extinct.

   (b) $\forall x \in \mathbb{R},\ (x > 0 \vee x < 0 \vee x = 0)$.

   (c) $\forall x \in \mathbb{R},\ (x \text{ is irrational} \to x \notin \mathbb{Z})$.

   (d) $\forall x \in L,\ x$ is not lazy.

   (e) $\forall x \in \mathbb{Z},\ x^2 \neq 2147581953$.

   (f) $\forall x \in \mathbb{R},\ -1 \neq x^2$.

2. (a) $\exists x \in X$ such that x has an answer.

   (b) $\exists x \in \mathbb{R}$ such that $x \in \mathbb{Q}$.

3. (a) **False.** Counterexample: take $x = \frac{1}{2}$. Then $x = \frac{1}{2}$ but $\frac{1}{x} = 2$, so $x \geq \frac{1}{x}$ is false.

   (b) **False.** Counterexample: take $a = 1$. Then $\frac{a-1}{a} = \frac{0}{1} = 0 \in \mathbb{Z}$.

   (c) **False.** Counterexample: take $n = m = 1$. Then $mn = 1$ but $m + n = 2$.

§7 — Negation of Quantified Statements

Epp 4th ed. pp. 108–117 · 5th ed. (metric) pp. 122–131. Lecture 6 (week 2). Notes: quantified-statements[191].

Problems

1. Write the negation of each of the following statements, and then determine whether the original or the negation is true:

   (a) $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$.

   (b) $\forall n \in \mathbb{Z}^+$, n is either prime or composite.

   (c) $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$.

2. Write down the negation of each of the following statements:

   (a) All fire engines are red.

   (b) Some apples are ripe.

   (c) A triangle with equal sides exists.

[191] courses/math1061/quantified-statements.pdf

Solutions

1. (a) **Original:** $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$. **Negation:** $\exists x \in \mathbb{R}$ such that $x^2 > 9$ and $x < 2$.

   The original statement is **false**. For instance, take $x = -4$. Then $x^2 > 9$ but $x \ngeq 2$.

   (b) **Original:** $\forall n \in \mathbb{Z}^+$, n is either prime or composite. **Negation:** $\exists n \in \mathbb{Z}^+$ such that n is neither prime nor composite.

   The original statement is **false**. For instance, consider $n = 1$, which is neither prime nor composite.

   (c) **Original:** $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$. **Negation:** $\forall x, y \in \mathbb{R}$, if $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ then $xy \notin \mathbb{Z}$.

   The original statement is **true**. For instance, take $x = \sqrt{2}$ and $y = \sqrt{2}$. Then $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$, but $xy = 2 \in \mathbb{Z}$.

2. (a) **Original:** All fire engines are red. **Negation:** There exists a fire engine which is not red.

   (b) **Original:** Some apples are ripe. **Negation:** All apples are not ripe.

   (c) **Original:** A triangle with equal sides exists. **Negation:** There does not exist a triangle with equal sides.

§8 — Statements with Multiple Quantifiers

Epp 4th ed. pp. 117–131 · 5th ed. (metric) pp. 131–146. Lecture 6 (week 2). Notes: quantified-statements[192].

Problems

1. Write down the negation of each of the following statements. Then determine whether the statement is true, or whether its negation is true.

   (a) $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$.

   (b) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$.

   (c) $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$.

   (d) $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$.

2. For each of the following English sentences:

[192] courses/math1061/quantified-statements.pdf

(a) For any rational number x and any negative integer y there exists a real number that is greater than the product of x and y.

(b) For every real number x, there is a real number y for which $3y = x$.

do the following:

i. Write the statement in symbolic form.

ii. Write the negation of the statement in symbolic form.

iii. Determine which of the statement or its negation is true.

Solutions

1. (a) **Original:** $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$. **Negation:** $\exists x \in \mathbb{Z}$ $\exists y \in \mathbb{Z}$ such that $\forall z \in \mathbb{Z}$, $z \neq x - y$.

The original statement is **true** (and the negation is false). For any given $x, y \in \mathbb{Z}$, choose $z = x - y \in \mathbb{Z}$.

(b) **Original:** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}$, $x^2 - xy - 2y^2 \neq 0$.

The original statement is **true** (and the negation is false). For any $x \in \mathbb{R}$, taking $y = \frac{x}{2}$ gives

$$x^2 - x\left(\frac{x}{2}\right) - 2\left(\frac{x}{2}\right)^2 = x^2 - \frac{x^2}{2} - 2 \cdot \frac{x^2}{4} = x^2 - \frac{x^2}{2} - \frac{x^2}{2} = 0.$$

(c) **Original:** $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$. **Negation:** $\forall x \in \mathbb{Z}^+$ $\exists y \in \mathbb{Z}^+$ such that $x < y$.

The **negation** is true (and the original is false). For any $x \in \mathbb{Z}^+$, take $y = x + 1$. Then y is an integer satisfying the inequality $x < y$.

(d) **Original:** $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$. **Negation:** $\exists r, s \in \mathbb{R}$ such that $rs \in \mathbb{Q}$ and ($r \notin \mathbb{Q}$ or $s \notin \mathbb{Q}$).

The **negation** is true (and the original is false). Take $r = \sqrt{2}$ and $s = \sqrt{2}$. Then $rs = 2 \in \mathbb{Q}$ but $r, s \notin \mathbb{Q}$.

2. (a) i. **Original:** $\forall x \in \mathbb{Q}$, $\forall y \in \mathbb{Z}^{<0}$, $\exists z \in \mathbb{R}$ s.t. $z > xy$.

ii. **Negation:** $\exists x \in \mathbb{Q}$ $\exists y \in \mathbb{Z}^{<0}$ s.t. $\forall z \in \mathbb{R}$, $z \leq xy$.

iii. The **original** statement is true. For any given $x \in \mathbb{Q}$ and $y \in \mathbb{Z}^{<0}$, take $z = xy + 1$. This is a real number satisfying the inequality $z > xy$.

(b) i. **Original:** $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}$ s.t. $3y = x$.

ii. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R},\ 3y \neq x$.

iii. The **original** statement is true. Given any $x \in \mathbb{R}$, choose $y = \frac{x}{3}$. This is a real number satisfying the equality $3y = x$.

§9 — Direct Proofs and Counterexamples

Epp 4th ed. pp. 145–163 · 5th ed. (metric) pp. 160–182. Lecture 7 (week 3). Notes: proof-techniques[193].

Problems

1. For each of the following statements, either prove the statement or disprove it using a counterexample.

   (a) The sum of any pair of even integers is even.

   (b) There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.

   (c) There is an even integer n such that $5n - 4$ is prime.

   (d) $\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

   (e) $\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.

2. Find a counterexample that disproves the following statement:

   $$\text{For all } x \in \mathbb{R},\ \lfloor x^2 \rfloor = \lfloor x \rfloor^2.$$

   (Recall that $\lfloor \cdot \rfloor$ denotes the floor function.)

3. Find the errors in the following proofs and rewrite the proof correctly. Here is a list of common errors made when writing proofs:

   - Arguing from examples
   - Using the same variable to mean two different things
   - Jumping to the conclusion
   - Assuming what is to be proved
   - Confusion between what is known and what is to be shown
   - Use of the word *any* instead of *some*
   - Misuse of the word *if*

[193] courses/math1061/proof-techniques.pdf

(a) The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

(b) If a and b are even integers, then $4a + 2b$ is even.

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

(c) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true.

(d) $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that $n^2 + 2n + 1$ is composite, so this means

$$n^2 + 2n + 1 = rs$$

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite.

Solutions

1. (a) **The sum of any pair of even integers is even.**

Proof. Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence

$$m + n = 2k + 2\ell = 2(k + \ell),$$

which is even. Therefore, the sum of any pair of even integers is even. □

(b) **There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.**

Proof. Consider the positive integers $a = 3$, $b = 4$, $c = 5$. Then $a^2 + b^2 = 9 + 16 = 25 = c^2$. □

(c) **There is an even integer n such that $5n - 4$ is prime.** This statement is **false**. We prove the negation: $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

Proof. Suppose that n is an even integer. Thus $n = 2k$ for some integer k. Hence

$$5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2).$$

By definition, this means that $5n - 4$ is even. The only even prime is 2. If $2(5k - 2) = 2$, then $5k - 2 = 1$ and hence $k = \frac{3}{5}$ which is not an integer. Therefore $5n - 4$ is not a prime number. □

(d) **$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.**

Proof. Suppose n is a positive integer and $n \geq 4$. Let us factor

$$2n^2 - 5n + 2 = (2n - 1)(n - 2).$$

Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers > 1. Hence the expression is composite for all $n \geq 4$. □

(e) **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** This statement is **false**. Take $x = 1$ and $y = -2$. Then $y^2 = 4 > x^2 = 1$, but $y = -2 \not> 1 = x$.

2. Take $x = \frac{3}{2}$. Then $\lfloor x^2 \rfloor = \lfloor \frac{9}{4} \rfloor = 2$, while $\lfloor x \rfloor^2 = \lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$. Hence $\lfloor x^2 \rfloor \neq \lfloor x \rfloor^2$, so the statement is false.

3. (a) **Statement.** The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. **[Error: using k for both m and n means that the statement is only proved when $m = n + 1$.]** Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

Correct proof. Let m be any odd integer and let n be any even integer. Then there exist $k, \ell \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2\ell$. Hence

$$m - n = (2k + 1) - 2\ell = 2(k - \ell) + 1,$$

which is an odd integer by definition. □

(b) **Statement.** If a and b are even integers, then $4a + 2b$ is even. **[Error: the proof forgets to state its assumptions.]**

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \quad \textbf{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

Correct proof. Suppose a and b are even integers. Then $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Therefore

$$4a + 2b = 4(2k) + 2(2j) = 8k + 4j = 2(4k + 2j).$$

Since $k, j \in \mathbb{Z}$, we have $(4k + 2j) \in \mathbb{Z}$ and so, by definition, $4a + 2b$ is even. □

(c) **Statement.** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true. **[Error: the proof argues from a single example, which cannot establish a universal statement. Moreover, the statement is false.]**

Correct disproof. The statement is false. As a counterexample, let $x = 0$. We know that $0 \cdot y = 0$ for all $y \in \mathbb{R}$ and so there is no real number y such that $0 \cdot y = 1$. □

(d) **Statement.** $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that n^2+2n+1 is composite, so this means

$n^2+2n+1 = rs$ **[Error: forgets to define r, s — e.g. for some $r, s \in \mathbb{Z}$]**

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite. **[Error: this is jumping to the conclusion without showing what needs to be shown. The expression we need to show (the definition of composite) has been given but it has not been shown.]**

Correct proof. Let $n \in \mathbb{Z}$ with $n > 0$. Then we have

$$n^2 + 2n + 1 = (n + 1)(n + 1).$$

Now since $0 < n < n^2 + 2n$, we must have that $1 < n + 1 < n^2 + 2n + 1$. So by letting $r = s = n + 1$ we have shown that

$$n^2 + 2n + 1 = rs$$

for integers $1 < r, s < n^2 + 2n + 1$. By definition this means $n^2 + 2n + 1$ is composite. □

Application — Applications of Proofs to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 74–80.*

Computer programs have been developed to automate the task of reasoning and proving theorems. Many of these programs make use of a rule of inference known as **resolution**. This rule of inference is based on the tautology

$$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r) \tag{1}$$

Resolution can be used to build automatic theorem proving systems.

To construct proofs using resolution as the only rule of inference, the hypotheses and conclusion must be expressed as **clauses**. Clauses are logical expressions which only feature disjunctions of variables or their negations (i.e. expressions which only use $\vee$, $\sim$, so they do not use $\wedge$, $\rightarrow$). To express any statement as a clause, we can use the laws of logical equivalence.

Application problems

1. (a) Using a truth table, show that expression (1) is a tautology.

   (b) Write the following expressions as clauses.

   i. $\sim (\sim r \wedge w)$

   ii. $r \rightarrow u$

   iii. $\sim (u \wedge w)$

   (c) Use resolution only to show that the following argument is valid:

   If it is raining, then Yvette has their umbrella. It is not the case that Yvette has their umbrella and gets wet. It is not the case that Yvette gets wet while it is not raining. Therefore, Yvette does not get wet.

Application solutions

1. (a) The truth table is

p	q	r	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	F	T	F	T	T
F	F	F	F	T	F	F	T

Since the last column is always T, the statement is a tautology.

(b) Clause forms:

i. $\sim (\sim r \wedge w) \equiv r \vee \sim w$ (by De Morgan's law and double negative law).

ii. $r \rightarrow u \equiv \sim r \vee u$ (by definition of implication).

iii. $\sim (u \wedge w) \equiv \sim u \vee \sim w$ (by De Morgan's law).

(c) Define the following variables:

r	it is raining
u	Yvette has their umbrella
w	Yvette gets wet

Then we can express the argument as

1. $r \rightarrow u$
2. $\sim (u \wedge w)$
3. $\sim (\sim r \wedge w) \therefore \sim w$

Using the equivalences in (b), we can rewrite this as

1.	$\sim r \vee u$	
2.	$\sim u \vee \sim w$	
3.	$r \vee \sim w$	
4.	$\sim r \vee \sim w$	From 1 and 2 by Resolution
5.	$\sim w$	From 3 and 4 by Resolution.

§10 — Proof by Contradiction

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 8 (week 3). Notes: proof-techniques[194].

Problems

1. Prove the following statement using a proof by contradiction:

   For integers a and b, if $6a + 3b$ is odd, then b is odd.

2. Use a proof by contradiction to prove the following statement:

   For all positive integers x and y, $x^2 - y^2 \neq 1$.

Solutions

1. **For integers a and b, if $6a + 3b$ is odd, then b is odd.**

   Proof. Suppose the statement is false, that is, suppose that there exist integers a and b for which $6a + 3b$ is odd and b is even.

   Since b is even, $b = 2k$ for some integer k. Thus

   $$6a + 3b = 6a + 3(2k) = 6a + 6k = 2(3a + 3k).$$

   Since $a, k \in \mathbb{Z}$, $3a + 3k \in \mathbb{Z}$ so $6a + 3b$ is even. This contradicts our assumption that $6a + 3b$ is odd, so our assumption was incorrect and hence the original statement is true. □

[194] courses/math1061/proof-techniques.pdf

2. **For all positive integers x and y, $x^2 - y^2 \neq 1$.**

   Proof. Suppose, for contradiction, that x and y are positive integers satisfying $x^2 - y^2 = 1$. Now, by factoring, we have

   $$1 = x^2 - y^2 = (x - y)(x + y).$$

   Since x and y are positive integers, we must have $x - y = 1$ and $x + y = 1$. This means $2x = 2$, so $x = 1$. But then we must have $y = 0$ which is not a positive integer; this is a contradiction. Therefore the original statement is true. □

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[195].

Problems

1. Use proof by contraposition to prove the following statement:

   For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

2. Prove the following statement:

   For any integer n, n^2 is odd if and only if n is odd.

   Use a direct proof for the reverse implication ($\Leftarrow$), and a proof by contraposition for the forward implication ($\Rightarrow$).

3. Use proof by contraposition to prove the following statement:

   For all integers x and y, if $x^2(y^2 - 2y)$ is odd then x and y are odd.

[195] courses/math1061/proof-techniques.pdf

Solutions

1. **For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.**

   Proof. We prove the contrapositive statement, which is:

   > For all integers a and b, if a is even or b is even, then $(ab)^2$ is even.

   Let a and b be integers and suppose a is even or b is even. Without loss of generality, suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ is even, and therefore $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, we know $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even by definition. □

2. **For any integer n, n^2 is odd if and only if n is odd.**

   Proof. To prove this "if and only if" statement, we must prove each of the following two statements:

   > ($\Leftarrow$) For any integer n, if n is odd, then n^2 is odd. ($\Rightarrow$) For any integer n, if n^2 is odd, then n is odd.

   ($\Leftarrow$) Let n be an integer and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Hence $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Since $k \in \mathbb{Z}$, we have $2k^2+2k \in \mathbb{Z}$ and hence n^2 is odd by definition.

   ($\Rightarrow$) The contrapositive is: for any integer n, if n is even, then n^2 is even. Let n be an integer and suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 = 4k^2 = 2(2k^2)$. Since $k \in \mathbb{Z}$, we have $2k^2 \in \mathbb{Z}$, so n^2 is even by definition.

   Therefore, for all integers n, n^2 is odd if and only if n is odd. □

3. **For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.**

   Proof. We will prove the contrapositive statement, which is:

   > For all integers x and y, if x is even or y is even, then $x^2(y^2-2y)$ is even.

   Let $x, y \in \mathbb{Z}$ and suppose x or y is even. We consider the cases of x even or y even individually.

   Case 1. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Hence

   $$x^2(y^2-2y) = (2k)^2(y^2-2y) = 2(2k^2)(y^2-2y).$$

   Since $k, y \in \mathbb{Z}$, we have $(2k^2)(y^2-2y) \in \mathbb{Z}$, and hence $x^2(y^2-2y)$ is even, by definition.

Case 2. Suppose y is even. Then $y = 2\ell$ for some $\ell \in \mathbb{Z}$. Hence

$$x^2(y^2 - 2y) = x^2((2\ell)^2 - 2(2\ell)) = 2(x^2(2\ell^2 - 2\ell)).$$

Since $x, \ell \in \mathbb{Z}$, we have $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$ and thus $x^2(y^2 - 2y)$ is even, by definition. □

§12 — Rational Numbers

Epp 4th ed. pp. 163–170 · 5th ed. (metric) pp. 183–190. Lecture 9 (week 3). Notes: rational-and-irrational-numbers[196].

Problems

1. Prove the following statement:

   For real numbers m and n, if m is irrational and n is rational, then $m - n$ is irrational.

2. Prove the following statement:

   For a real number r, if $2r^2 - 3r$ is irrational, then r is irrational.

3. Prove the following statement:

   For all real numbers r, s, n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrati

4. Recall that $\sqrt{2}$ is irrational. Consider the statement

   For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.

   (a) Write down the negation of the statement.

   (b) Use a proof by contradiction to prove the statement.

[196] courses/math1061/rational-and-irrational-numbers.pdf

Solutions

1. **For real numbers m and n, if m is irrational and n is rational, then $m-n$ is irrational.**

   Proof. Let m and n be real numbers and suppose (for a contradiction) that m is an irrational number and n is rational, but $m-n$ is rational. Since n is rational, we have $n=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $m-n$ is rational, we have $m-n=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

   Notice that $m=(m-n)+n$. Hence

   $$m=(m-n)+n=\frac{c}{d}+\frac{a}{b}=\frac{bc+ad}{bd}.$$

   Since $a,b,c,d\in\mathbb{Z}$ we have $bc+ad\in\mathbb{Z}$ and $bd\in\mathbb{Z}$. Further, since $b\neq 0$ and $d\neq 0$, we have $bd\neq 0$. Thus, by definition, m is rational. But this contradicts the assumption that m is irrational. □

2. **For a real number r, if $2r^2-3r$ is irrational, then r is irrational.**

   Proof. We prove the contrapositive statement: for a real number r, if r is rational, then $2r^2-3r$ is rational.

   Let r be a real number and suppose $r\in\mathbb{Q}$. Then $r=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. So

   $$2r^2-3r=2\left(\frac{a}{b}\right)^2-3\left(\frac{a}{b}\right)=\frac{2a^2-3ab}{b^2}.$$

   Since $a,b\in\mathbb{Z}$, we have $2a^2-3ab\in\mathbb{Z}$ and $b^2\in\mathbb{Z}$. Further, $b^2\neq 0$ because $b\neq 0$. This means $2r^2-3r$ is rational, by definition. □

3. **For all real numbers r, s, and n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrational.**

   Proof. Suppose, for a contradiction, that the statement is false. Then there exist real numbers r, s and n such that r is an irrational number, s is rational, n is a positive integer, but $n(r-s)$ is rational. Since s is rational, $s=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $n(r-s)$ is rational, we have $n(r-s)=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

Now,

$$\begin{aligned} r - s &= n(r-s)\left(\frac{1}{n}\right) \quad \text{noting that } n \neq 0 \\ r - s &= \frac{c}{d} \cdot \frac{1}{n} \\ r &= s + \frac{c}{d} \cdot \frac{1}{n} \\ &= \frac{a}{b} + \frac{c}{dn} \\ &= \frac{adn + bc}{bdn} \end{aligned}$$

Since $a, b, c, d \in \mathbb{Z}$, we have $adn + bc \in \mathbb{Z}$ and $bdn \in \mathbb{Z}$. Further, since $b \neq 0$, $d \neq 0$ and $n \neq 0$, we have $bdn \neq 0$. This means r is rational, by definition, which is a contradiction. □

4. **For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.**

   (a) **Negation:** There exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

   (b)

   Proof. Suppose, for a contradiction, that the original statement is false. Then there exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$. Since r is rational, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and since $r \neq 0$, we have $a \neq 0$. Since we have assumed $r\sqrt{2}$ is rational, $r\sqrt{2} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Now

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \left(r\sqrt{2}\right)\left(\frac{1}{r}\right) = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad}.$$

   Since $a, b, c, d \in \mathbb{Z}$, we know $bc \in \mathbb{Z}$ and $ad \in \mathbb{Z}$. Further, since $a \neq 0$ and $d \neq 0$, we have $ad \neq 0$. Thus, by definition, $\sqrt{2}$ is rational. However, this is a contradiction, as $\sqrt{2}$ is irrational. Thus, the original statement is true. □

§13 — Divisibility

Epp 4th ed. pp. 170–179 · 5th ed. (metric) pp. 190–199. Lecture 10 (week 4). Notes: divisibility-and-factorisation[197].

[197] courses/math1061/divisibility-and-factorisation.pdf

Problems

1. Find the unique factorisation (in standard form) of the integer 27 720.
2. Prove or disprove the statement: for any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.
3. Prove the following statements.
   (a) If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.
   (b) The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.
4. Use proof by contradiction to prove this statement:

$$\text{For all integers } c, d \text{ and } e, \text{ if } c \mid d \text{ and } c \nmid e, \text{ then } c \nmid (d+e).$$

Solutions

1. By repeated division, we have $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.
2. **For any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.** The statement is **true**, and we will prove it.

   Proof. Let m, n, and q be non-zero integers. Assume $m \mid n$ and $n \mid q$. Then, by definition, there exist integers a, b such that

   $$n = ma \quad \text{and} \quad q = nb.$$

   Then observe

   $$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2b).$$

   Since $a^2b \in \mathbb{Z}$, we conclude that $m^2 \mid nq$. □
3. (a) **If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.**

   Proof. Let k be even and m be odd. Then $k = 2a$ and $m = 2b+1$ for some $a, b \in \mathbb{Z}$. Hence

   $$(k+2)^2 = (2a+2)^2 = 4(a+1)^2 \quad \text{and} \quad (m-3)^2 = (2b-2)^2 = 4(b-1)^2.$$

   Therefore

   $$(k+2)^2-(m-3)^2 = 4\big[(a+1)^2-(b-1)^2\big].$$

   Since $a, b \in \mathbb{Z}$ we have $(a+1)^2-(b-1)^2 \in \mathbb{Z}$ so $4 \mid \big[(k+2)^2-(m-3)^2\big]$. □

(b) **The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.**

Proof. Let n and $n+1$ be two consecutive integers. The difference between their cubes is

$$(n+1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n+1) + 1.$$

Now whether n is odd or even (so whatever integer n is), one of n, $n+1$ will be odd and the other one will be even. Thus the product $n(n+1)$ is even.

Since $n(n+1)$ is even, write $n(n+1) = 2t$ for some $t \in \mathbb{Z}$. Then

$$(n+1)^3 - n^3 = 3(2t) + 1 = 6t + 1 \equiv 1 \pmod 6.$$

Hence the remainder is 1 upon division by 6. □

4. **For all integers c, d and e, if $c \mid d$ and $c \nmid e$, then $c \nmid (d+e)$.**

Proof. Suppose for a contradiction that the statement is false. Then there exist integers c, d and e such that $c \mid d$ and $c \nmid e$ and $c \mid (d+e)$.

Now $c \mid d$ means that $d = cx$ for some integer x. And $c \mid (d+e)$ means that $d + e = cy$ for some integer y.

Hence $d + e = cx + e = cy$, so $e = cy - cx = c(y - x)$, and we have $y - x \in \mathbb{Z}$, because x and y are both integers. Thus $c \mid e$, a contradiction. So the original statement is true. □

§14 — Modular Arithmetic

Epp 4th ed. pp. 482–485 · 5th ed. (metric) pp. 528–531. Lecture 11 (week 4). Notes: modular-arithmetic[198].

Problems

1. Prove the following statement:

   If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.

2. (a) Evaluate $58 \operatorname{div} 11$ and $58 \bmod 11$.

[198] courses/math1061/modular-arithmetic.pdf

(b) Find integers q and r, with $0 \leqslant r < d$ and $n = dq + r$, in the case that $n = -95$ and $d = 11$.

3. (a) An integer n, when divided by 7, leaves remainder 4. What is the remainder (between 0 and 6 inclusive) when $3n$ is divided by 7?

   (b) When the integer m is divided by 11, the remainder 9 is left. What remainder is left when $4m$ is divided by 22?

4. Prove or disprove the following statements.

   (a) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

   (b) For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.

Solutions

1. **If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.**

   Proof. Fix $y \in \mathbb{Z}$. By the division algorithm, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

   $$y^2 = (5m + r)^2 = 25m^2 + 10mr + r^2 \equiv r^2 \pmod 5.$$

   Let us compute the possible values for r^2 mod 5:

   $$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

   Thus $y^2 \equiv 0, 1$, or $4 \pmod 5$, and never 2 or 3. □

2. (a) Since $58 = 11 \cdot 5 + 3$ with $0 \leq 3 < 11$, we have

   $$58 \operatorname{div} 11 = 5 \quad \text{and} \quad 58 \bmod 11 = 3.$$

   (b) We want $-95 = 11q + r$ with $0 \leq r < 11$. Taking $q = -9$ gives

   $$11(-9) = -99 \quad \Rightarrow \quad -95 = -99 + 4 = 11(-9) + 4,$$

   so $q = -9$ and $r = 4$.

3. (a) If n leaves remainder 4 upon division by 7, then $n = 7k + 4$ for some integer k. Hence

$$3n = 21k + 12 = 7(3k + 1) + 5,$$

so the remainder when $3n$ is divided by 7 is **5**. (The source PDF prints this step as $7(3k) + 5$, which equals $21k + 5$, not $21k + 12$ — the quotient is $3k + 1$, as above. The answer of 5 is unaffected.)

(b) If m leaves remainder 9 upon division by 11, then $m = 11k + 9$ for some integer k. Then

$$4m = 44k + 36 = 22(2k + 1) + 14,$$

so the remainder when $4m$ is divided by 22 is **14**.

4. (a) **For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** The statement is **false**. For a counterexample, take $x = \frac{3}{2}$. Then

$$\lfloor x^2 \rfloor = \left\lfloor \frac{9}{4} \right\rfloor = 2 \quad \text{but} \quad \lfloor x \rfloor^2 = \left\lfloor \frac{3}{2} \right\rfloor^2 = 1^2 = 1.$$

(b) **For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.** The statement is **true**.

Proof. Let n be an odd integer, so $n = 2k + 1$ for some integer k. Then

$$\frac{n^2}{4} = \frac{(2k+1)^2}{4} = \frac{4k^2 + 4k + 1}{4} = k(k+1) + \frac{1}{4},$$

so $\left\lfloor \frac{n^2}{4} \right\rfloor = k(k+1)$. Moreover, notice

$$\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = \left(\frac{2k}{2}\right)\left(\frac{2k+2}{2}\right) = k(k+1).$$

Hence $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$ for all odd integers n. □

§15 — The Euclidean Algorithm

Epp 4th ed. pp. 220–224 · 5th ed. (metric) pp. 250–254. Lecture 12 (week 4). Notes: gcd-lcm-and-euclidean-algorithm[199].

[199] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

Problems

1. Use the Euclidean Algorithm to determine $\gcd(14, 3003)$.
2. Compute
   (a) $\operatorname{lcm}(12, 18)$
   (b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
   (c) $\operatorname{lcm}(2800, 6125)$
3. Prove that for all positive integers a and b, we have

$$\gcd(a, b) = \operatorname{lcm}(a, b) \iff a = b.$$

4. Prove that for all positive integers a and b, we have

$$a \mid b \iff \operatorname{lcm}(a, b) = b.$$

5. (a) Use the Euclidean algorithm to determine $\gcd(931, 301)$. Show your working.
   (b) Write down the unique prime factorisation of 931 in standard form.
   (c) How many positive divisors does 931 have? (Hint: use part (b).)
6. (a) Using the Euclidean algorithm, compute $\gcd(116, 88)$. Show your working.
   (b) Using your answer to part (a), compute $\operatorname{lcm}(116, 88)$.

Solutions

1. We apply the Euclidean Algorithm:

$$3003 = 14 \cdot 214 + 7, \qquad 14 = 7 \cdot 2 + 0.$$

   Hence $\gcd(14, 3003) = 7$.

2. (a) We factor $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$ so $\operatorname{lcm}(12, 18) = 2^2 \cdot 3^2 = 36$.
   (b) Using the maximum exponents of each prime, we have

$$\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

   (c) We factor $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$. Thus

$$\operatorname{lcm}(2800, 6125) = 2^4 \cdot 5^3 \cdot 7^2 = 98000.$$

3. **For all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.**

   Proof. Let a and b be positive integers.

   ($\Longleftarrow$) It is clear that if $a = b$ then $\gcd(a, b) = \operatorname{lcm}(a, b)$.

   ($\Longrightarrow$) Assume $\gcd(a, b) = \operatorname{lcm}(a, b)$. Denoting $g = \gcd(a, b)$, we have $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$.

   Now notice gm and gn have no common prime factors beyond those in g, so the least common multiple uses all primes from both m and n. Therefore

   $$\operatorname{lcm}(a, b) = gmn.$$

   Now, we have $g = gmn$. Therefore $mn = 1$, and so $m = n = 1$. This lets us conclude $a = b$. □

4. **For all positive integers a and b, $a \mid b$ if and only if $\operatorname{lcm}(a, b) = b$.**

   Proof. Let us denote $g = \gcd(a, b)$ so that $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$. As explained in the previous question, we have

   $$\operatorname{lcm}(a, b) = gmn.$$

   ($\Longrightarrow$) If $a \mid b$, then $gm \mid gn$, hence $m \mid n$. Since $\gcd(m, n) = 1$, we conclude $m = 1$. Therefore $\operatorname{lcm}(a, b) = gmn = gn = b$.

   ($\Longleftarrow$) If $\operatorname{lcm}(a, b) = b$, then $gmn = gn$ which means $m = 1$. Therefore $a = gm = g$ and so $a \mid b$. □

5. (a) Using the Euclidean Algorithm:

   $$\begin{aligned} 931 &= 301 \cdot 3 + 28 \\ 301 &= 28 \cdot 10 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

   Hence $\gcd(931, 301) = 7$.

   (b) Since $\gcd(931, 301) = 7$, we know $7 \mid 931$, and we have $931 = 7 \cdot 133$. The number 133 has prime factorisation $7 \cdot 19$. Therefore the unique prime factorisation of 931 is $7^2 \cdot 19$.

(c) We have $931 = 7^2 \cdot 19^1$ from part (b). Any divisor of 931 must have a prime factorisation of the form $7^a \cdot 19^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. Thus the number of positive divisors is

$$(2 + 1)(1 + 1) = 6.$$

(There are 3 choices for the exponent a and 2 choices for the exponent b.)

6. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 116 &= 88 \cdot 1 + 28 \\ 88 &= 28 \cdot 3 + 4 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Hence $\gcd(116, 88) = 4$.

(b) Using $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{Z}^+$,

$$\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{\gcd(116, 88)} = \frac{116 \cdot 88}{4} = 116 \cdot 22 = 2552.$$

Application — Trace Tables for Algorithms

Not assessable for MATH1061. For reference, see S. Epp, Discrete Mathematics with Applications, *Section 4.8 (4th edition) or Section 4.10 (5th edition), Brooks/Cole, Belmont, CA.*

The following pseudo-code describes the **Division Algorithm**, with annotations to explain what each step is doing.

Input: a (a non-negative integer), d (a positive integer). This algorithm will take two inputs, a and d, and will find the quotient $a \operatorname{div} d$ and the remainder $a \bmod d$.

Algorithm body:

```
r := a          -- defining our variables
q := 0
                -- starting with a, repeatedly subtract lots of d until we reach
                -- a number less than d; each round adds 1 to the quotient count
while r >= d,
    r := r - d
    q := q + 1
end while
```

Output: q, r. Once we have obtained a number less than d, we are finished. The output q is the quotient ($a \operatorname{div} d$) and the output r is the remainder ($a \bmod d$).

The following pseudo-code describes the **Euclidean Algorithm**, with annotations to explain what each step is doing.

Input: A, B (integers with $A > B \geq 0$).

Algorithm body:

```
a := A          -- defining our variables
b := B
r := B
                -- if b /= 0, compute a mod b (call the algorithm above for this
                -- step) and set r to be this value; replace a with b and b with r
                -- and repeat until b = 0
while b /= 0,
    r := a mod b
    a := b
    b := r
end while
gcd := a
```

Output: gcd (a positive integer).

A **trace table** keeps track of the value of each variable at each step of an algorithm. For example, the trace table for the Division Algorithm with input variables $a = 19$ and $d = 4$ is:

Variable / iteration	0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

Output: $q = 4$, $r = 3$.

Application problems

1. Construct a trace table to trace the action of the Division Algorithm for the following inputs.

   (i) $a = 26$, $d = 7$

(ii) $a = 15$, $d = 6$

2. Construct a trace table to trace the action of the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$.

Application solutions

1. (i) Trace table for the Division Algorithm with $a = 26$, $d = 7$:

Variable / iteration	0	1	2	3
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

Output: $q = 3$, $r = 5$.

(ii) Trace table for the Division Algorithm with $a = 15$, $d = 6$:

Variable / iteration	0	1	2
a	15		
d	6		
r	15	9	3
q	0	1	2

Output: $q = 2$, $r = 3$.

2. Trace table for the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$:

Variable / iteration	0	1	2	3	4	5
A	1001					
B	871					
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Output: gcd = 13.

§16 — Sequences

Epp 4th ed. pp. 227–244 · 5th ed. (metric) pp. 258–275. Lecture 13 (week 5).

Problems

1. Write down the first four terms in the sequence defined by $a_k = \dfrac{k}{10+k}$ for $k = 1, 2, \ldots$.
2. Consider the sequences $a_k = 2k + 1$ and $b_k = (k-1)^3 + k + 2$ where $k = 0, 1, 2, \ldots$. Show that the first three terms of these sequences are identical, but that their fourth terms differ.
3. (a) Find an explicit formula for a sequence c_n whose first six terms are $-1, 1, -1, 1, -1, 1$.
   (b) Find an explicit formula for a sequence d_n whose first six terms are $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$.
4. (a) Write $(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)$ in summation notation.
   (b) Evaluate $\displaystyle\prod_{i=1}^{5}(-1)^i \cdot i$.
   (c) Write $(y-1)(y^2-2)(y^3-3)(y^4-4)$ in product notation.
   (d) Evaluate $\displaystyle\sum_{j=1}^{n}(-1)^j\frac{1}{2^j}$ when $n = 5$.

Solutions

1. We have

$$a_1 = \frac{1}{11}, \qquad a_2 = \frac{2}{12} = \frac{1}{6}, \qquad a_3 = \frac{3}{13}, \qquad a_4 = \frac{4}{14} = \frac{2}{7}.$$

2. We compute

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 5, \quad a_3 = 7;$$

$$b_0 = (-1)^3+0+2 = 1, \quad b_1 = 0^3+1+2 = 3, \quad b_2 = 1^3+2+2 = 5, \quad b_3 = 2^3+3+2 = 13.$$

Hence the first three terms agree ($a_0 = b_0$, $a_1 = b_1$ and $a_2 = b_2$), but the fourth terms differ ($a_3 = 7$ while $b_3 = 13$).

3. (a) One explicit formula is

$$c_n = (-1)^n \qquad n = 1, 2, 3, ...$$

(b) The denominators are square numbers, so an explicit formula is

$$d_n = \frac{n}{(n+1)^2} \qquad n = 1, 2, 3, ...$$

4. (a) We have

$$(x^2 - 1) + (2x^3 - 1) + (3x^4 - 1) + (4x^5 - 1) + (5x^6 - 1) = \sum_{k=1}^{5} \left(kx^{k+1} - 1\right).$$

(b) We have

$$\prod_{i=1}^{5}(-1)^i \cdot i = \left(\prod_{i=1}^{5}(-1)^i\right)\left(\prod_{i=1}^{5} i\right) = (-1)^{1+2+3+4+5} \cdot 5! = (-1)^{15} \cdot 120 = -120.$$

(c) We have

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} \left(y^k - k\right).$$

(d) When $n = 5$, we have

$$\sum_{j=1}^{5}(-1)^j \frac{1}{2^j} = -\frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} = -\frac{11}{32}.$$

§17 — Mathematical Induction

Epp 4th ed. pp. 244–268 · 5th ed. (metric) pp. 275–301. Lecture 13 (week 5).

Problems

1. Use mathematical induction to prove the following statements.

   (a) For every positive integer n, $n(n+1)$ is even.

   (b) For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.

   (c) For all integers $n \geq 7$, $3^n < n!$.

   (d) For each integer $n \geq 1$,

   $$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

   (e) For each integer $n \geq 0$, $1 + 4n \leq 5^n$.

Solutions

1. (a) **For every positive integer n, $n(n+1)$ is even.**

   Proof. Let $P(n)$ be the predicate "$n(n+1)$ is even".

   Basis: when $n = 1$, $n(n+1) = 2$ which is even, so $P(1)$ is true.

   (The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

   Inductive hypothesis: suppose that for some integer $k \geq 1$, $P(k)$ is true. Thus $k(k+1) = 2a$ for some integer a.

   Now consider $n = k + 1$. Then

   $$(k+1)(k+2) = k(k+1) + 2(k+1) = 2a + 2(k+1) = 2(a+k+1).$$

   Since a and k are integers, $a + k + 1$ is an integer, so $(k+1)(k+2)$ is even and $P(k+1)$ is true.

   Thus, by the principle of mathematical induction, $n(n+1)$ is even for every positive integer n. □

   (b) **For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.**

Proof. Let $P(n)$ be the predicate $6 \mid (n^3 - n)$.

Basis: when $n = 2$, $n^3 - n = 8 - 2 = 6$. Since $6 \mid 6$, $P(2)$ is true.

(The inductive step is to show that for all integers $k \geq 2$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose that for some integer $k \geq 2$, $P(k)$ is true. Thus $k^3 - k = 6a$ for some integer a.

Now consider $n = k + 1$. Then

$$(k+1)^3-(k+1) = k^3+3k^2+3k+1-k-1 = k^3-k+3k^2+3k = 6a+3k(k+1).$$

For the integer k, $k(k+1)$ is even from part (a), so let $k(k+1) = 2b$ for some integer b. Hence $(k+1)^3 - (k+1) = 6a + 3(2b) = 6(a+b)$. Thus $6 \mid ((k+1)^3 - (k+1))$ and so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $n^3 - n$ is a multiple of 6 for each integer $n \geq 2$. □

(c) **For all integers $n \geq 7$, $3^n < n!$.**

Proof. Let $P(n)$ be the predicate $3^n < n!$.

Basis: $P(7)$ is the statement $3^7 < 7!$. The left-hand side is $3^7 = 2187$ and the right-hand side is $7! = 5040$, so $P(7)$ holds.

(The inductive step is to show that for all integers $k \geq 7$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: let $k \geq 7$ be an integer and assume that $P(k)$ is true; that is $3^k < k!$. We will now show that $P(k+1)$ holds, so we will show $3^{k+1} < (k+1)!$.

Taking the right-hand side, we have

$$\begin{aligned}
(k+1)! &= (k+1) \cdot k! \\
&> (k+1) \cdot 3^k && \text{by the inductive hypothesis} \\
&> 3 \cdot 3^k && \text{since } k \geq 7 \\
&= 3^{k+1}
\end{aligned}$$

Hence $P(k+1)$ is true.

Thus by the principle of mathematical induction, for all integers $n \geq 7$, $3^n < n!$. □

(d) **For each integer $n \geq 1$, $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.**

Proof. Let $P(n)$ be the predicate

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Basis: consider $n = 1$. We have $\sum_{i=1}^{1} i^3 = 1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ so $P(1)$ is true.

(The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(k)$ is true. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

Now consider $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 && \text{(splitting off the last term)} \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 && \text{by the inductive hypothesis} \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{(k+1)^2}{4}(k^2 + 4(k+1)) \\
&= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\
&= \frac{(k+1)^2}{4}(k+2)^2
\end{aligned}$$

Thus $P(k+1)$ is true.

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for every integer $n \geq 1$. □

(e) **For each integer $n \geq 0$, $1 + 4n \leq 5^n$.**

Proof. Let $P(n)$ be the predicate $1 + 4n \leq 5^n$.

Basis: when $n = 0$ we have $1 + 4 \cdot 0 \leq 5^0$, so $P(0)$ is true.

(The inductive step is to show that for all integers $k \geq 0$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 0$ is an integer and $P(k)$ is true; that is, $1 + 4k \leq 5^k$.

Now consider $n = k + 1$. Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned} 1 + 4(k+1) &= 1 + 4k + 4 \\ &\leq 5^k + 4 && \text{by the inductive hypothesis} \\ &\leq 5^k + 4 \cdot 5^k && \text{since } k \geq 0 \text{ so } 5^k \geq 1 \\ &= 5(5^k) \\ &= 5^{k+1} \end{aligned}$$

so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $1 + 4n \leq 5^n$ for every integer $n \geq 0$. □

§18 — Strong Induction and the Well Ordering Principle

Epp 4th ed. pp. 268–279 · 5th ed. (metric) pp. 301–314. Lecture 14 (week 5).

Problems

1. Consider the statement

   For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.

   (a) Prove the statement using the well-ordering principle.

   (b) Prove the statement using strong mathematical induction.

2. The Lucas sequence $a_1, a_2, a_3, ...$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Use strong mathematical induction to prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

3. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Use strong mathematical induction to prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.

Solutions

1. **For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.**

   (a)

Proof (using the well-ordering principle). Consider the set of counterexamples

$$S = \{\, n \in \mathbb{Z}^{\geq 2} : \text{there do not exist integers } a, b \geq 0 \text{ with } n = 2a + 3b \,\}.$$

If S is empty, we are done. Otherwise, by the well-ordering principle, S has a least element. Let us call it N.

Notice that $2 \notin S$ because $2 = 2 \cdot 1 + 3 \cdot 0$, and $3 \notin S$ because $3 = 2 \cdot 0 + 3 \cdot 1$. Also $4 \notin S$ because $4 = 2 \cdot 2 + 3 \cdot 0$. Hence $N \geq 5$. By minimality of N, we must have $N - 2 \notin S$. Therefore there exist integers $a, b \geq 0$ such that

$$N - 2 = 2a + 3b.$$

In other words, we have

$$N = 2(a + 1) + 3b.$$

This means $N \notin S$, contradicting the assumption that $N \in S$. Hence S is empty, and the statement holds for all $n \geq 2$. $\square$

(b)

Proof (using strong induction). Let $P(n)$ be the predicate: "there exist integers $a, b \geq 0$ such that $n = 2a + 3b$."

Basis: we have

$$2 = 2 \cdot 1 + 3 \cdot 0, \qquad 3 = 2 \cdot 0 + 3 \cdot 1, \qquad 4 = 2 \cdot 2 + 3 \cdot 0,$$

so $P(2)$, $P(3)$, $P(4)$ are true.

(The inductive step is to show that for every integer $k \geq 4$, if $P(2), P(3), \ldots, P(k)$ are all true then $P(k + 1)$ is true.)

Inductive hypothesis: suppose $k \geq 4$ is an integer and assume $P(m)$ is true for every integer $m = 2, 3, \ldots, k$.

Consider $n = k + 1$. Since $k \geq 4$, we have $k - 1 \geq 3$, so by the inductive hypothesis $P(k - 1)$ is true. Thus there exist $a, b \geq 0$ such that

$$k - 1 = 2a + 3b.$$

Adding 2 gives

$$k + 1 = 2(a + 1) + 3b,$$

so $P(k + 1)$ holds. $\square$

2. **The Lucas sequence** $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $P(n)$ be the predicate $a_n \leqslant \left(\frac{7}{4}\right)^n$.

Basis: when $n = 1$, $a_1 = 1 \leqslant \left(\frac{7}{4}\right)^1 = 1\frac{3}{4}$ is true, so $P(1)$ is true. When $n = 2$, $P(2)$ holds because $a_2 = 3 \leqslant \left(\frac{7}{4}\right)^2 = \frac{49}{16} = 3\frac{1}{16}$.

(The inductive step is to show that for every integer $k \geq 1$, if $P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and that $P(m)$ is true for all m with $1 \leq m \leq k$.

Now consider $P(k+1)$, which we want to prove holds. We have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&\leqslant \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} && \text{by the inductive hypothesis} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right) \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right) \\
&\leqslant \left(\frac{7}{4}\right)^{k-1}\left(\frac{49}{16}\right) && \text{noting } \tfrac{11}{4} = \tfrac{44}{16} < \tfrac{49}{16} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 \\
&= \left(\frac{7}{4}\right)^{k+1}.
\end{aligned}$$

Hence $P(k+1)$ holds. Therefore, by the principle of strong mathematical induction, $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all integers $n \geqslant 1$. □

3. **Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.**

Proof. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Let $P(n)$ be the predicate "a_n is an integer."

Basis: $P(0)$ holds since $a_0 = x^0 + \frac{1}{x^0} = 2$. $P(1)$ holds since $a_1 = x + \frac{1}{x}$, which is an integer by assumption.

(The inductive step is to show that for every integer $k \geq 1$, if $P(0), P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(m)$ holds for all integers $m = 0, 1, \ldots, k$.

We now aim to show that $P(k+1)$ is true. Notice that

$$\begin{aligned} a_1 a_k &= \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) \\ &= \left(x^{k+1} + \frac{1}{x^{k+1}}\right) + \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_{k+1} + a_{k-1}. \end{aligned}$$

Therefore $a_{k+1} = a_1 a_k - a_{k-1}$. By the inductive hypothesis, a_k and a_{k-1} are integers, and a_1 is an integer, so a_{k+1} is an integer. Hence $P(k+1)$ holds.

Therefore, by the principle of strong mathematical induction, a_n is an integer for all $n \geq 0$. □

§19 — Recursive Definitions

Epp 4th ed. pp. 290–304 · 5th ed. (metric) pp. 325–340. Lecture 15 (week 6).

Problems

1. Define the sequence $b_1 = 2$, $b_2 = 6$ and

$$b_k = b_{k-1} + b_{k-2} + \gcd(b_{k-1}, b_{k-2})$$

for all $k \geq 3$. Use strong induction to prove b_n is even for all $n \geq 1$.

2. A sequence is defined by $a_1 = 2$ and

$$a_k = k(a_{k-1} + k - 1)$$

for all integers $k \geq 2$. Use mathematical induction to prove a_n is even for all $n \geq 1$.

3. Recursively define the set S of binary strings as follows.

   (a) *(Base rule)* $1 \in S$.

   (b) *(Recursion rule)* If $s \in S$ then $0s \in S$ and $1s \in S$ (e.g. if $s = 1$ then $0s = 01$).

   (c) *(Restriction rule)* No other strings lie in S besides those given by the rules above.

   What are the strings contained in S arising from the first three applications of the recursive rule?

Solutions

1. *Proof.* Let $P(n)$ be the predicate "b_n is even".

   Base case. The base cases are $n = 1, 2$. We have $b_1 = 2$ and $b_2 = 6$ so $P(1)$ and $P(2)$ are true.

   Inductive hypothesis. Assume $P(m)$ is true for all integers m with $1 \leq m \leq k$, where $k \geq 2$ is an integer. That is, we assume $b_1, b_2, \ldots, b_k$ are all even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. b_{k+1} is even. Using the recursive definition, we have

   $$b_{k+1} = b_k + b_{k-1} + \gcd(b_k, b_{k-1}).$$

   By the inductive hypothesis, b_k and b_{k-1} are even, so $2 \mid b_k$ and $2 \mid b_{k-1}$, hence $2 \mid \gcd(b_k, b_{k-1})$ as well. Therefore each term on the right-hand side is even, so their sum b_{k+1} is even. Thus $P(k+1)$ holds.

   Therefore, b_n is even for all integers $n \geq 1$. □

2. *Proof.* Let $P(n)$ be the predicate "a_n is even".

   Base case. The base case is $n = 1$. We have $a_1 = 2$, which is even, so $P(1)$ is true.

   Inductive hypothesis. Assume $P(k)$ is true for some integer $k \geq 1$. That is, assume a_k is even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. a_{k+1} is even. By the recursive definition, we have

   $$a_{k+1} = (k+1)(a_k + (k+1) - 1) = (k+1)(a_k + k).$$

   Note that a_k is even by the inductive hypothesis. We split into cases:

   - If k is even, then $a_k + k$ is even, hence a_{k+1} is even.
   - If k is odd, then $k+1$ is even, hence a_{k+1} is even.

   In all cases, a_{k+1} is even, so $P(k+1)$ is true.

   Therefore, a_n is even for all integers $n \geq 1$. □

3. By the base rule, we only know $1 \in S$.

   First application of the recursive rule:

   $$01 \in S, \qquad 11 \in S.$$

   Second application of the recursive rule:

$$001 \in S, \quad 101 \in S, \quad 011 \in S, \quad 111 \in S.$$

Third application of the recursive rule:

$$0001 \in S, \quad 1001 \in S, \quad 0101 \in S, \quad 1101 \in S,$$
$$0011 \in S, \quad 1011 \in S, \quad 0111 \in S, \quad 1111 \in S.$$

§20 — Solving Recurrence Relations

Epp 4th ed. pp. 304–328 · 5th ed. (metric) pp. 340–364. Lecture 16 (week 6).

Problems

1. Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that

$$a_n = 5a_{n-1} - 6a_{n-2}$$

for all integers $n \geq 2$.

2. Let $\{b_n\}_{n\geq 0}$ be the sequence defined by

$$b_0 = 2, \qquad b_1 = 5, \qquad \text{and} \qquad b_k = 2b_{k-1} - b_{k-2} \text{ for each integer } k \geq 2.$$

   (a) Write down the values of $b_0, b_1, b_2, b_3, b_4, b_5$.

   (b) Based on your answers for part (a), guess an explicit formula for this sequence.

   (c) Prove that your guess from part (b) is correct.

3. Let T_n be a sequence defined by $T_1 = 1$ and

$$T_{n+1} = 1 + (T_1 \times T_2 \times T_3 \times \cdots \times T_n)$$

for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.

4. Consider the Fibonacci sequence defined recursively by

$$\begin{aligned} a_0 &= 0 \\ a_1 &= 1 \\ a_n &= a_{n-2} + a_{n-1} \qquad \text{for all integers } n \geq 2. \end{aligned}$$

Use strong mathematical induction to prove the explicit formula

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

for all integers $n \geq 0$, where $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. (You may use the fact that $\phi^2 = \phi + 1$ and $\psi^2 = \psi + 1$.)

Solutions

1. **Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$.**

Proof. For $n \geq 2$, we have $n - 2 \geq 0$ so all three terms a_n, a_{n-1} and a_{n-2} are defined in the given formula. Then,

$$\begin{aligned} 5a_{n-1} - 6a_{n-2} &= 5\left(2^{n-1} + 5 \cdot 3^{n-1}\right) - 6\left(2^{n-2} + 5 \cdot 3^{n-2}\right) \\ &= \left(5 \cdot 2^{n-1} - 6 \cdot 2^{n-2}\right) + \left(25 \cdot 3^{n-1} - 30 \cdot 3^{n-2}\right) \\ &= (10 - 6)2^{n-2} + (75 - 30)3^{n-2} \\ &= 4 \cdot 2^{n-2} + 45 \cdot 3^{n-2} \\ &= 2^n + 5 \cdot 3^n \\ &= a_n. \end{aligned}$$

Hence $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. □

2. (a)

$$\begin{aligned} b_0 &= 2 \\ b_1 &= 5 \\ b_2 &= 2(5) - 2 = 8 \\ b_3 &= 2(8) - 5 = 11 \\ b_4 &= 2(11) - 8 = 14 \\ b_5 &= 2(14) - 11 = 17 \end{aligned}$$

(b) Guess that $b_n = 3n + 2$ for each integer $n \geq 0$.

(c)

Proof. The guess gives $b_0 = 3(0) + 2 = 2$ and $b_1 = 3(1) + 2 = 5$ so it gives the correct initial conditions. Now we substitute the guess into the recurrence relation. The LHS of the recurrence relation is $b_k = 3k + 2$. The RHS of the recurrence relation is

$$\begin{aligned} 2b_{k-1} - b_{k-2} &= 2(3(k-1)+2) - (3(k-2)+2) \\ &= 2(3k-1) - (3k-4) \\ &= 6k - 2 - 3k + 4 \\ &= 3k + 2 \end{aligned}$$

So the guess also satisfies the recurrence relation. Thus the guess is correct. □

Alternative proof (by strong induction). Let $P(n)$ be the predicate $b_n = 3n + 2$.

Basis: $b_0 = 2$ from the recursive definition and $3(0) + 2 = 2$ so $P(0)$ is true. $b_1 = 5$ from the recursive definition and $3(1) + 2 = 5$ so $P(1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are true.

Now

$$\begin{aligned} b_{k+1} &= 2b_k - b_{k-1} && \text{by the rec. rel. since } k+1 \geq 2 \\ &= 2(3k+2) - (3(k-1)+2) && \text{since } P(k) \text{ and } P(k-1) \text{ are true} \\ &= 6k + 4 - (3k - 1) \\ &= 3k + 5 \\ &= 3(k+1) + 2 \end{aligned}$$

So $P(k+1)$ is true. Therefore, by the principle of (strong) mathematical induction, the guess is correct for this recursively defined sequence. □

3. **Let T_n be a sequence defined by $T_1 = 1$ and $T_{n+1} = 1 + (T_1 \times \cdots \times T_n)$ for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.**

Proof. We can prove this simply by applying the recursive formula twice, once for T_{n+1} and once for T_n:

$$\begin{aligned} T_{n+1} &= 1 + (T_1 \cdot T_2 \cdot T_3 \cdots T_n) && \text{by the recursive definition} \\ &= 1 + T_n \cdot (T_1 \cdot T_2 \cdot T_3 \cdots T_{n-1}) \\ &= 1 + T_n \cdot (T_n - 1) && \text{since } T_n = 1 + (T_1 \cdots T_{n-1}) \text{ by rec. def.} \\ &= 1 + (T_n)^2 - T_n \\ &= (T_n)^2 - T_n + 1. \end{aligned}$$

Note that both applications of the recursive definition are valid, since $n-1 \geq 1$. $\square$

4. **Fibonacci explicit formula.**

Proof. Let $P(n)$ be the predicate

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}.$$

Basis. The base cases are $n = 0, 1$, which are true because

$$\frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = a_0,$$

and

$$\frac{\phi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = a_1.$$

Inductive hypothesis. Now suppose that for some integer $m \geq 1$, we have that $P(i)$ is true for all $0 \leq i \leq m$. In particular, $P(m)$ and $P(m-1)$ are true, that is,

$$a_m = \frac{\phi^m - \psi^m}{\sqrt{5}} \qquad \text{and} \qquad a_{m-1} = \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}}.$$

We need to show that $P(m+1)$ is true. That is, we aim to show

$$a_{m+1} = \frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}}.$$

Starting with the right-hand side of $P(m+1)$, we have

$$\begin{aligned}
\frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}} &= \frac{\phi^2\phi^{m-1} - \psi^2\psi^{m-1}}{\sqrt{5}} \\
&= \frac{(\phi+1)\phi^{m-1} - (\psi+1)\psi^{m-1}}{\sqrt{5}} && \text{since } \phi^2 = \phi + 1 \text{ and } \psi^2 = \psi + 1 \\
&= \frac{(\phi^m + \phi^{m-1}) - (\psi^m + \psi^{m-1})}{\sqrt{5}} \\
&= \frac{\phi^m - \psi^m}{\sqrt{5}} + \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}} \\
&= a_m + a_{m-1} && \text{by the inductive hypothesis} \\
&= a_{m+1} && \text{by definition.}
\end{aligned}$$

Hence $P(m+1)$ is true. $\square$

§21 — Set Theory Definitions

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Define the sets

$$\begin{aligned} V &= \{x \in \mathbb{Z} \mid 2 \leqslant x \leqslant 11 \text{ and } x \text{ is odd}\}, \\ X &= \{x \in \mathbb{Z} \mid -1 \leqslant x \leqslant 4\}, \\ Y &= \{2, 3, 7, 9\}, \\ Z &= \{x \in \mathbb{Z} \mid x \neq 0\}. \end{aligned}$$

   Write down the following sets, listing their elements and using brackets as appropriate.

   (a) $V \cap X$. (b) $V \cup Y$. (c) $X \cap Z$.

   (b) $X \cap (Z - Y)$. (e) $(X \cup Y) \cap V$. (f) $X \cup (Y \cap V)$.

2. For each of the following sets, write down its elements and then state the size of the set; that is, find $|A|$, $|B|$, $|C|$ and $|D|$.

   (a) $A = \{x \in \mathbb{Z} \mid \exists\, i \in \mathbb{Z} \text{ such that } x = 1 + (-1)^i\}$.

   (b) $B = \{y \in \mathbb{Z} \mid -8 < y \leqslant -5\}$.

   (c) $C = \{s \in \mathbb{Z} \mid s^2 + 1 = 0\}$.

   (d) $D = \{t \in \mathbb{Z} \mid t^4 = 1\}$.

3. Define the sets $A = \{0, 1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ and $C = \{1, 2, 4, 5, 7\}$. List the elements of the set

$$R = ((A - B) \cap (A - C)) \cup (B \cap C \cap A).$$

4. Are the following statements true or false? Justify in one or two sentences.

   (a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{\emptyset\} \in \{\{\emptyset\}\}$

   (b) $\emptyset \subseteq \{x\}$ (e) $\emptyset \in \{x\}$

Solutions

1. (a) $V \cap X = \{3\}$

   (b) $V \cup Y = \{2, 3, 5, 7, 9, 11\}$

   (c) $X \cap Z = \{-1, 1, 2, 3, 4\}$

   (d) $X \cap (Z - Y) = \{-1, 1, 4\}$

   (e) $(X \cup Y) \cap V = \{3, 7, 9\}$

   (f) $X \cup (Y \cap V) = \{-1, 0, 1, 2, 3, 4, 7, 9\}$

2. (a) Note that $(-1)^i$ is either $+1$ or -1 (according as i is even or odd). So x is either $1 + 1$ or $1 - 1$, that is, 2 or 0. So $A = \{2, 0\}$ and $|A| = 2$.

   (b) $B = \{-7, -6, -5\}$, so $|B| = 3$.

   (c) If $s^2 + 1 = 0$, we have $s^2 = -1$, and there are no such real numbers s, let alone integers! So $C = \emptyset$ and $|C| = 0$.

   (d) $D = \{-1, 1\}$, since $t^4 = 1$ with $t \in \mathbb{Z}$ implies $t = \pm 1$. Hence $|D| = 2$.

3. We have $A - B = \{0, 1, 2\}$ and $A - C = \{0, 3\}$, so $(A - B) \cap (A - C) = \{0\}$. Also $B \cap C \cap A = \{4\}$. Thus $R = \{0\} \cup \{4\} = \{0, 4\}$.

4. (a) **True:** $\{x\}$ is the set whose only element is x, so $x \in \{x\}$.

   (b) **True:** every set is a subset of itself, so $\{x\} \subseteq \{x\}$.

   (c) **True:** $\{\{\emptyset\}\}$ has the single element $\{\emptyset\}$, so $\{\emptyset\} \in \{\{\emptyset\}\}$.

   (d) **True:** $\emptyset \subseteq S$ for every set S, in particular $\emptyset \subseteq \{x\}$.

   (e) **False** (in general): $\emptyset \in \{x\}$ would require $\emptyset = x$.

Application — Computer Representations of Sets

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 134–138.*

There are various ways to represent sets using a computer. One such method involves the use of binary strings.

If we fix a finite universal set U with an arbitrary ordering, for example $U = \{a_1, a_2, \ldots, a_n\}$, we can represent subsets of U using binary strings of length n. A 1 in the ith position of the string indicates that element a_i is in the subset and a 0 indicates it is not.

For example if $U = \{1, 2, 3\}$ then the string 000 represents the empty set, 101 represents the subset $\{1, 3\}$ and 111 represents the entire set U.

The set operations union and intersection can be computed at the level of binary strings by utilising the bitwise OR and AND operations. The union of two sets corresponds to the bitwise OR operation on the strings and the intersection corresponds to bitwise AND.

Application problems

1. Define the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   (a) Express each of the following subsets of U using binary strings:

   i. $\{3, 4, 5\}$

   ii. $\{1, 3, 6, 10\}$

   iii. $\{a \in U \mid a \text{ is prime}\}$.

   (b) Using the same U, find the set represented by the following strings:

   i. 1111001111

   ii. 0101111000

   iii. 1000000001

   (c) Use binary strings to compute the following set operations.

   i. $\{1, 3, 4, 6, 10\} \cap \{2, 3, 6, 9, 10\}$

   ii. $\{2, 4, 6, 8\} \cup \{3, 4, 5\}$

Application solutions

1. (a) i. 0011100000

   ii. 1010010001

   iii. 0110101000 — the primes in U are $2, 3, 5, 7$. (The source PDF prints 1010111000 here, which decodes to $\{1, 3, 5, 6, 7\}$ and is not the set of primes; the string above is the correct one.)

   (b) i. $\{1, 2, 3, 4, 7, 8, 9, 10\}$

   ii. $\{2, 4, 5, 6, 7\}$

   iii. $\{1, 10\}$

   (c) i. 1011010001 AND 0110010011 = 0010010001, so the intersection is $\{3, 6, 10\}$.

   ii. 0101010100 OR 0011100000 = 0111110100, so the union is $\{2, 3, 4, 5, 6, 8\}$.

§22 — More Definitions and Examples of Sets

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Let $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$. List the elements of the following sets.
   (a) $A \cap C$
   (b) $(A \cup C) - B$
   (c) $(A \times B) \cap (A \times C)$
   (d) $\mathcal{P}(B \cap C)$
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\}$
2. Are the following statements true or false?
   (a) $\mathbb{Q} \in \mathbb{R}$.
   (b) $\{1, 2\} \subseteq \mathbb{Z}$.
   (c) $\{-3, 0\} \subseteq \mathcal{P}(\mathbb{Z})$.
   (d) $\{(1, 2), (0, 1)\} \in \mathbb{Z} \times \mathbb{Z}$.
3. Let $X = \mathcal{P}(\emptyset)$ and $Y = \mathcal{P}(\mathcal{P}(\emptyset))$. List the elements of each of the following sets.
   (a) X (b) Y (c) $X \cap Y$ (d) $X \cup Y$
4. Define sets $S = \{3, 5\}$ and $T = \{2, 3, 7\}$. Are the following statements true or false?
   (a) $S \subseteq T$
   (b) $\emptyset \in \mathcal{P}(S)$
   (c) $\emptyset \in T$
   (d) $(3, 3, 3) \in S \times T$

Solutions

1. (a) $A \cap C = \emptyset$.
   (b) $(A \cup C) - B = \{1, 4\}$.
   (c) $(A \times B) \cap (A \times C) = \{(1, 3), (2, 3)\}$.
   (d) $\mathcal{P}(B \cap C) = \{\emptyset, \{3\}\}$.
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\} = \{\emptyset, \{2\}\}$.
2. (a) **False.** ($\mathbb{Q}$ is a *subset* of $\mathbb{R}$, not an element of it.)
   (b) **True.**
   (c) **False.** (The elements of $\mathcal{P}(\mathbb{Z})$ are sets of integers; -3 and 0 are integers, not sets.)
   (d) **False.** (It is a *subset* of $\mathbb{Z} \times \mathbb{Z}$, not an element — the elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs.)
3. (a) $X = \mathcal{P}(\emptyset) = \{\emptyset\}$.
   (b) $Y = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
   (c) $X \cap Y = \{\emptyset\}$.
   (d) $X \cup Y = \{\emptyset, \{\emptyset\}\}$.
4. (a) **False.** ($5 \in S$ but $5 \notin T$.)
   (b) **True.** (The empty set is an element of every power set.)
   (c) **False.** (T's elements are 2, 3 and 7.)
   (d) **False.** (The elements of $S \times T$ are ordered *pairs*, not triples.)

§23 — Properties of Sets

Epp 4th ed. pp. 352–366 · 5th ed. (metric) pp. 391–407. Lecture 18 (week 7).

Problems

1. (a) Use the element method to prove that for all sets A and B

$$A \cup (B - A) = A \cup B.$$

   (b) Use the element method to prove that for all sets X, Y and Z,

$$(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset.$$

   (c) Use set identities to prove that for all sets A, B and C

$$(A - B) - C = A - (B \cup C).$$

2. Prove or disprove the following:

   (a) For all sets A and B, we have $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

   (b) For all sets A and B, we have $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.

   (c) There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

   (d) Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$.

3. Let A, B and C be sets. Prove that

$$A - (B \cup C) = (A - B) - C.$$

Solutions

1. (a) **For all sets A and B, $A \cup (B - A) = A \cup B$.**

   Proof. First we show that $A \cup (B - A) \subseteq A \cup B$.

   Consider an arbitrary element $x \in A \cup (B - A)$. Then we know $x \in A$ or $x \in B - A$. This means $x \in A$, or $x \in B$ and $x \notin A$. If $x \in A$, then $x \in A \cup B$. Similarly if $x \in B - A$, then it must be in B and so $x \in A \cup B$. In either case, we have $x \in A \cup B$, thus $A \cup (B - A) \subseteq A \cup B$.

   Now we show that $A \cup B \subseteq A \cup (B - A)$.

   Let $x \in A \cup B$, then $x \in A$ or $x \in B$ or it is in both A and B. If $x \in A$, then $x \in A \cup (B - A)$. If $x \notin A$ then $x \in B$ since $x \in A \cup B$. So we have that $x \in B$ and $x \notin A$, hence $x \in B - A$ and thus $x \in A \cup (B - A)$. This proves that $A \cup B \subseteq A \cup (B - A)$, and together this proves that $A \cup B = A \cup (B - A)$. $\square$

(b) **For all sets X, Y and Z, $(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset$.**

Proof. Assume that $(X - Z) \cap (Y - Z) \cap (X - Y) \neq \emptyset$.

So let $x \in (X - Z) \cap (Y - Z) \cap (X - Y)$. Then, in particular, $x \in Y - Z$ and $x \in X - Y$. The former implies $x \in Y$, but the latter implies $x \notin Y$. No such x exists. Therefore the set is empty. □

(c) **For all sets A, B and C, $(A - B) - C = A - (B \cup C)$.**

Proof. Using $A - B = A \cap B^c$, $(S - T) = S \cap T^c$, and De Morgan's law, we have

$$(A-B)-C = (A\cap B^c)\cap C^c = A\cap(B^c\cap C^c) = A\cap(B\cup C)^c = A-(B\cup C). \qquad \square$$

2. (a) **For all sets A and B, $\mathcal{P}(A\cup B) = \mathcal{P}(A)\cup\mathcal{P}(B)$. False.** Counterexample: $A = \{1\}$, $B = \{2\}$. Then

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \neq \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}.$$

(b) **For all sets A and B, $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$. True.**

($\Longleftarrow$) If $A = B$ then clearly $\mathcal{P}(A) = \mathcal{P}(B)$.

($\Longrightarrow$) We next show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Suppose (for a contradiction) that $\mathcal{P}(A) = \mathcal{P}(B)$ but $A \neq B$. Then (without loss of generality), there exists an element x in A that is not in B. Therefore, there is an element $\{x\}$ in $\mathcal{P}(A)$ that is not in $\mathcal{P}(B)$. Therefore $\mathcal{P}(A) \neq \mathcal{P}(B)$ — a contradiction. Thus, for all sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$. □

(c) **There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. False.**

No such set exists. The power set of any set must contain the empty set — that is, $\emptyset \in \mathcal{P}(A)$, where A is any set. Also, the power set of any set of size n has cardinality 2^n. The power set above contains 7 elements, and there does not exist any integer n such that $2^n = 7$.

(d) **Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$. True.**

First note that if $A = \emptyset$ then $A \times B = A \times C = \emptyset$ and the statement is true. Also, if $B = \emptyset$ then $A \times B = \emptyset$ and $\emptyset \subseteq A \times C$ for any C, so the statement is true.

Suppose A, B and C are non-empty sets with $B \subseteq C$. Thus if $b \in B$, then $b \in C$. Consider any element $(a, b) \in A \times B$, where $a \in A$ and $b \in B$. Since

$b \in B$, $b \in C$. As such, $a \in A$ and $b \in C$ for all a or b, so $(a, b) \in A \times C$. Therefore $A \times B \subseteq A \times C$. □

3. **For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.**

   Proof Option 1. For any x, we have

   $$x \in A - (B \cup C) \iff x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge (x \notin B) \wedge (x \notin C).$$

   Also, we have

   $$x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff (x \in A \wedge x \notin B) \wedge x \notin C.$$

   The statements on the right-hand side are equivalent. Hence $A - (B \cup C) = (A - B) - C$. □

   Proof Option 2.

   $$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c && \text{by the Set Difference Law} \\ &= A \cap (B^c \cap C^c) && \text{by De Morgan's law} \\ &= (A \cap B^c) \cap C^c && \text{by Associative law} \\ &= (A - B) \cap C^c && \text{by the Set Difference Law} \\ &= (A - B) - C && \text{by the Set Difference Law} \quad \square \end{aligned}$$

§24 — Functions Defined on General Sets

Epp 4th ed. pp. 383–396 · 5th ed. (metric) pp. 425–439. Lecture 18 (week 7).

Problems

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 1$.
   (a) What is the domain, codomain and range of f?
   (b) What is the image of $\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$ under f?
   (c) What is the preimage of $\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}$ under f?
2. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$ be sets. Define $f : X \to Y$ by the arrow diagram

   $$1 \mapsto v, \qquad 3 \mapsto s, \qquad 5 \mapsto v$$

   (the elements t and u of Y receive no arrows).

(a) Write the domain of f and the co-domain of f.

(b) Determine $f(1)$, $f(3)$, and $f(5)$.

(c) Determine the range of f.

(d) Is 3 an inverse image of s? Is 1 an inverse image of u?

(e) What is the inverse image of s? of u? of v?

(f) Represent f as a set of ordered pairs.

3. Let D be the set of all finite subsets of $\mathbb{Z}^+$. Consider the function $T : \mathbb{Z}^+ \to D$ defined by $T(n) := \{d \mid d \in \mathbb{Z}^+ \text{ and } d \text{ divides } n\}$. Find the following:

(a) $T(1)$ (b) $T(15)$ (c) $T(17)$ (d) $T(5)$ (e) $T(18)$ (f) $T(21)$

4. Let S be the set of all strings of a's and b's.

(a) Define the function $f : S \to \mathbb{Z}$ by

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s, & \text{if } s \text{ contains an } a, \\ 0, & \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

(b) Define the function $g : S \to S$ by

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

Solutions

1. (a) The domain is $\mathbb{R}$, the codomain is $\mathbb{R}$, and the range is $[-1, \infty)$.

(b) $f(\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}) = [-1, 3]$.

(c) $f^{-1}(\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} = [-2, -1] \cup [1, 2]$.

2. (a) The domain is $X = \{1, 3, 5\}$ and the codomain is $Y = \{s, t, u, v\}$.

(b) $f(1) = v$, $f(3) = s$, $f(5) = v$.

(c) $\text{range}(f) = \{s, v\}$.

(d) **Yes**, 3 is an inverse image of s. **No**, 1 is not an inverse image of u.

(e) $f^{-1}(s) = \{3\}$, $f^{-1}(u) = \emptyset$, $f^{-1}(v) = \{1, 5\}$.

(f) $f = \{(1, v), (3, s), (5, v)\}$.

3. (a) $T(1) = \{1\}$.

(b) $T(15) = \{1, 3, 5, 15\}$.

(c) $T(17) = \{1, 17\}$.

(d) $T(5) = \{1, 5\}$.

(e) $T(18) = \{1, 2, 3, 6, 9, 18\}$.

(f) $T(21) = \{1, 3, 7, 21\}$.

4. (a) $f(aba) = 0$, $f(bbab) = 2$, $f(b) = 0$, $\text{range}(f) = \mathbb{Z}^{\geq 0}$.

(b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, $\text{range}(g) = S$.

§25 — one-to-one, Onto, and Inverse Functions

Epp 4th ed. pp. 397–416 · 5th ed. (metric) pp. 439–461. Lecture 19 (week 7).

Problems

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \left\lfloor \dfrac{1 - 6n}{3} \right\rfloor$.

(a) Is f one-to-one?

(b) Is f onto?

(c) Is f bijective?

(d) Prove or disprove that for all $m, n \in \mathbb{Z}$, we have $f(mn) = f(m)f(n)$.

2. Define the set $A = \{0, 1, 2, 3, 4\}$ and the functions $f : A \to A$ and $g : A \to A$ by

$$f(a) = (a + 4)^2 \pmod 5, \qquad g(a) = (a^2 + 3a + 1) \pmod 5.$$

Is $f = g$?

3. Consider the function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f((m, n)) = 2^m 3^n$.

(a) Determine $f((3, 1))$.

(b) Determine the pre-image of $\{36\}$.

(c) Prove f is one-to-one.

4. Consider the function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x^2 \rfloor$.

   (a) What is the image $f([-1, 1])$?

   (b) What is the preimage $f^{-1}(\{1\})$?

   (c) Is f one-to-one?

   (d) Is f onto?

   (e) Is f bijective?

Solutions

1. First, we note that, for $n \in \mathbb{Z}$,

$$f(n) = \left\lfloor \frac{1-6n}{3} \right\rfloor = \left\lfloor -2n + \frac{1}{3} \right\rfloor = -2n$$

   since $-2n \in \mathbb{Z}$ and $\frac{1}{3} \in [0, 1)$.

   (a) **Yes.** If $f(m) = f(n)$ then $-2m = -2n$, hence $m = n$. Therefore f is one-to-one.

   (b) **No.** Since $f(n) = -2n$ we see that f never maps to any odd integer; for example, there is no integer w with $f(w) = 1$. Therefore f is not onto.

   (c) **No**, f is not a bijection. (It is injective but not surjective.)

   (d) This is **false**; take $m = n = 1$. Then $f(mn) = -2$ but $f(m)f(n) = 4$.

2. **Yes.** First note f and g have the same domain and codomain. This means we just need to show $f(a) = g(a)$ for all $a \in A$. Notice that we have

$$(a+4)^2 = a^2 + 8a + 16 \equiv a^2 + 3a + 1 \pmod 5,$$

   so $f(a) = g(a)$ for all $a \in A$, and hence $f = g$.

3. (a) $f((3, 1)) = 2^3 3^1 = 24$.

   (b) $36 = 2^2 3^2$, so $f((m, n)) = 36$ if and only if $(m, n) = (2, 2)$. Hence $f^{-1}(\{36\}) = \{(2, 2)\}$.

   (c) If $f((m, n)) = f((m', n'))$, then $2^m 3^n = 2^{m'} 3^{n'}$, so $2^{m-m'} = 3^{n'-n}$. By unique prime factorisation, this forces $m - m' = 0$ and $n' - n = 0$. That is, $m = m'$ and $n = n'$, and hence $(m, n) = (m', n')$. So f is one-to-one.

4. (a) Note that if $x \in [-1, 1]$ then $x^2 \in [0, 1]$. This means we have $\lfloor x^2 \rfloor \in \{0, 1\}$. Both values occur because $\lfloor 0^2 \rfloor = 0$ and $\lfloor 1^2 \rfloor = 1$. Thus $f([-1, 1]) = \{0, 1\}$.

(b) $f^{-1}(\{1\}) = \{x \in \mathbb{R} : 1 \leq x^2 < 2\} = (-\sqrt{2}, -1] \cup [1, \sqrt{2})$.

(c) **No**, f is not one-to-one. For example, $f\left(\frac{1}{2}\right) = 0 = f\left(-\frac{1}{2}\right)$ but $\frac{1}{2} \neq -\frac{1}{2}$.

(d) **No**, f is not onto since $f(x) = \lfloor x^2 \rfloor \geq 0$ for all x. This means, for instance, that -1 is not in the image of f.

(e) **No**, f is not bijective.

§26 — Composition of Functions

Epp 4th ed. pp. 416–427 · 5th ed. (metric) pp. 461–472. Lecture 20 (week 7).

Problems

1. Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^3 - 1$ and $g(x) = x + 5$.
   (a) Determine the functions $(g \circ f)(x)$ and $(f \circ g)(x)$.
   (b) Is $g \circ f$ a bijection?
2. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(x) = 2\lfloor x + 1 \rfloor$.
   (a) What is the range of f?
   (b) Is f one-to-one?
   (c) Is f onto?
   (d) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = 2x - 1$. Determine the composition $(g \circ f)(x)$.
   (e) Calculate $(g \circ f)\left(-\frac{3}{4}\right)$.
   (f) What is the range of $g \circ f$?
3. Let f and g be functions. Prove or disprove the following statements:
   (a) If f and $f \circ g$ are one-to-one, then g is one-to-one.
   (b) If f and $f \circ g$ are onto, then g is onto.

Solutions

1. (a) We have

$$(g \circ f)(x) = g(x^3 - 1) = x^3 + 4$$

and

$$(f \circ g)(x) = f(x + 5) = (x + 5)^3 - 1 = x^3 + 15x^2 + 75x + 124.$$

(b) **No**, $g \circ f$ is not a bijection. The map $x \mapsto x^3 + 4$ is one-to-one on $\mathbb{Z}$, but it is not onto (e.g. 0 is not in its image since $x^3 = -4$ has no integer solution).

2. (a) The range is a subset of the even integers because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. If $2m$ is an even integer then $f(m - 1) = 2\lfloor m - 1 + 1 \rfloor = 2m$, so the range is the set of all even integers.

(b) **No**, f is not one-to-one. For example,

$$f(0) = 2\lfloor 0 + 1 \rfloor = 2\lfloor 1 \rfloor = 2 \times 1 = 2, \quad \text{and}$$
$$f\left(\tfrac{1}{2}\right) = 2\left\lfloor \tfrac{1}{2} + 1 \right\rfloor = 2\left\lfloor \tfrac{3}{2} \right\rfloor = 2 \times 1 = 2,$$

but $0 \neq \frac{1}{2}$.

(c) **No**, f is not onto since $\text{range}(f) \neq \mathbb{Z}$ (e.g. there is no $x \in \mathbb{Q}$ such that $f(x) = 1$ because 1 is odd).

(d) We have

$$(g \circ f)(x) = g(f(x)) = 2(2\lfloor x + 1 \rfloor) - 1 = 4\lfloor x + 1 \rfloor - 1.$$

(e) We have

$$(g \circ f)\left(-\frac{3}{4}\right) = 4 \cdot 0 - 1 = -1.$$

(f) The range is a subset of $\{4n - 1 \mid n \in \mathbb{Z}\}$ because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. This *is* the range because, given an integer $4n - 1$, we have $f(n - 1) = 4\lfloor n - 1 + 1 \rfloor - 1 = 4n - 1$. Note that you can also write the range as $\{n \in \mathbb{Z} \mid n \equiv -1 \pmod 4\}$ which is the same as $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 4\}$.

3. (a) The statement is **true**.

Proof. Suppose that f and $f \circ g$ are one-to-one functions. Suppose for a contradiction that g is not one-to-one. Thus there exist two distinct elements in the domain of g, say x_1 and x_2, for which $g(x_1) = g(x_2)$. Let $g(x_1) = y = g(x_2)$. Thus $f(g(x_1)) = f(y) = f(g(x_2))$, but $x_1 \neq x_2$, which contradicts the fact that $f \circ g$ is one-to-one. Therefore g must be one-to-one. □

(b) The statement is **false**.

Counterexample. Consider the functions $g : \{1\} \to \{2, 3\}$ defined by $g(1) = 2$, and $f : \{2, 3\} \to \{4\}$ defined by $f(2) = 4$ and $f(3) = 4$. Then f is onto, and $f \circ g$ is onto (since $f \circ g : \{1\} \to \{4\}$ and $f(g(1)) = 4$). However, g is not onto. □

§27 — Cardinalities

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 21 (week 8).

Problems

1. Let $A = \{-2, -1, 0, 1\}$ and $B = \{3, 4, 5, 6\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.
2. Prove that $|\{1, 2, 3\}| \leq |\mathbb{Z}|$ by providing an appropriate injective (one-to-one) function.
3. Consider the intervals

$$[6, 12] = \{x \in \mathbb{R} \mid 6 \leq x \leq 12\} \quad \text{and} \quad (6, 12) = \{x \in \mathbb{R} \mid 6 < x < 12\}.$$

   Prove that $|[6, 12]| \leq |(6, 12)|$ by providing an appropriate injective (one-to-one) function.
4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.

Solutions

1. Define the function $f : A \to B$ by

$$f(-2) = 3, \qquad f(-1) = 4, \qquad f(0) = 5, \qquad f(1) = 6.$$

   Then f is bijective, hence $|A| = |B|$.
2. Define the function $g : \{1, 2, 3\} \to \mathbb{Z}$ by $g(1) = 1$, $g(2) = 2$, and $g(3) = 3$. Then g is injective (one-to-one), so $|\{1, 2, 3\}| \leq |\mathbb{Z}|$.

3. Define $h : [6, 12] \to (6, 12)$ by

$$h(x) = \frac{x}{2} + 4.$$

For each $x \in [6, 12]$ we have

$$\begin{aligned} \frac{6}{2} + 4 \leq h(x) &\leq \frac{12}{2} + 4 \\ 7 \leq h(x) &\leq 10. \end{aligned}$$

Thus h is indeed a function from $[6, 12]$ to $(6, 12)$, and h has range $[7, 10] \subseteq (6, 12)$.

Suppose $x, y \in [6, 12]$ and $h(x) = h(y)$. Then $\frac{x}{2} + 4 = \frac{y}{2} + 4$, so $x = y$. Therefore h is injective (one-to-one).

Thus $|[6, 12]| \leq |(6, 12)|$.

4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$.

Consider the function $f : A \to B$ where $f(x) = 2x + 5$. Since $x \geq -1$, $f(x) = 2x + 5 \geq 2(-1) + 5 = 3$, and since $x \leq 1$, $f(x) = 2x + 5 \leq 2(1) + 5 = 7$. Also each value of x gives a unique value of $2x + 5$. Thus f is a function with the correct domain and codomain.

We now prove that f is one-to-one. Suppose that $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Thus $2x_1 + 5 = 2x_2 + 5$, and so $x_1 = x_2$. Thus f is one-to-one.

We now prove that f is onto. Suppose $y \in [3, 7]$. Let $x = \frac{y-5}{2}$. Since $y \leq 7$, we have $x \leq 1$ and since $y \geq 3$, we have $x \geq -1$. So $x \in [-1, 1]$. Furthermore $f(x) = f\left(\frac{y-5}{2}\right) = 2\left(\frac{y-5}{2}\right) + 5 = y - 5 + 5 = y$. Thus f is onto.

Hence f is a bijection and so $|A| = |B|$.

§28 — Countable and Uncountable Sets

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 22 (week 8).

Note that this content will not be assessed in MATH1061.

Problems

1. Determine whether each of the following sets is countable or uncountable.
   (a) $\{1, 2, \ldots, n\}$.
   (b) $\mathbb{Z} \times \mathbb{Z}$.
   (c) $\mathbb{Q} \times \mathbb{Q}$.
   (d) $\mathbb{Z} \times \mathbb{Z} \times \cdots$ (infinitely many copies of $\mathbb{Z}$).
2. (a) Is $|\mathbb{Z}| = |\mathbb{Q}|$?
   (b) Is $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$?
   (c) Is $|\mathbb{R}| = |\mathbb{Q} \times \mathbb{Q}|$?
3. (a) Show that the union of a countable number of countable sets is countable.
   (b) Show that the set of all finite binary strings is countable.
   (c) Use (a) to show that the set of all irrational numbers is uncountable.

Solutions

1. (a) The set is **countable** because the function $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ defined by $f(i) = i$ is injective.
   (b) The set $\mathbb{Z} \times \mathbb{Z}$ is **countable**. Define the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ by

$$f(a,b) = \begin{cases} 2^a 3^b, & a > 0,\ b > 0, \\ 5^{-a} 7^{-b}, & a < 0,\ b < 0, \\ 11^a 13^{-b}, & a > 0,\ b < 0, \\ 17^{-a} 19^b, & a < 0,\ b > 0, \\ 23^b, & a = 0,\ b > 0, \\ 29^a, & a > 0,\ b = 0, \\ 31^{-b}, & a = 0,\ b < 0, \\ 37^{-a}, & a < 0,\ b = 0, \\ 1, & (a,b) = (0,0). \end{cases}$$

   We claim f is injective. Suppose $f(a,b) = f(c,d)$. By unique prime factorisation, the set of primes dividing $f(a,b)$ and the set of primes dividing $f(c,d)$ must be equal. Hence (a,b) and (c,d) lie in the same case. Again, by unique prime factorisation, the corresponding exponents must agree, so $a = c$ and $b = d$. Therefore f is injective.

(c) The set $\mathbb{Q} \times \mathbb{Q}$ is **countable**. First define an injection $e : \mathbb{Z} \to \mathbb{N}$ by

$$e(z) = \begin{cases} 2z, & z \geq 0, \\ -2z - 1, & z < 0. \end{cases}$$

Next define an injection $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$c(m, n) = 2^m 3^n.$$

Write each rational in lowest terms with positive denominator: $x = \frac{p}{q}$, $y = \frac{r}{s}$ with $p, r \in \mathbb{Z}$ and $q, s \in \mathbb{N}$. Define $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$ by

$$F\left(\frac{p}{q}, \frac{r}{s}\right) = 2^{\,c(e(p),\, q)}\, 3^{\,c(e(r),\, s)}.$$

If $F\left(\frac{p}{q}, \frac{r}{s}\right) = F\left(\frac{p'}{q'}, \frac{r'}{s'}\right)$, then by unique prime factorisation we get $c(e(p), q) = c(e(p'), q')$ and $c(e(r), s) = c(e(r'), s')$. Since c is injective, we have $e(p) = e(p')$, $q = q'$, $e(r) = e(r')$, $s = s'$. Moreover, since e is injective, we have $p = p'$ and $r = r'$. Therefore $\frac{p}{q} = \frac{p'}{q'}$ and $\frac{r}{s} = \frac{r'}{s'}$, so F is injective.

(d) The set $\mathbb{Z} \times \mathbb{Z} \times ...$ is **not countable**. We will prove this by giving an injection $\mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$.

For each $x \in \mathbb{R}$, write $x = n + r$ with $n = \lfloor x \rfloor \in \mathbb{Z}$ and $r \in [0, 1)$. Choose the unique decimal expansion of r that does not end with an infinite tail of 9's. Write this decimal expansion as

$$r = 0.d_1 d_2 d_3 \cdots, \qquad d_k \in \{0, 1, \ldots, 9\}.$$

Then define the function $\iota : \mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$ by

$$\iota(x) = (n, d_1, d_2, d_3, \ldots) \in \mathbb{Z} \times \mathbb{Z} \times \cdots.$$

This is injective; if $\iota(x) = \iota(y)$ then the decimals of x and y are equal, so $x = y$.

2. (a) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Q}$ are countable and infinite.

   (b) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are countable and infinite.

   (c) **No.** $\mathbb{Q} \times \mathbb{Q}$ is countable, while $\mathbb{R}$ is uncountable.

3. (a) Let $A_1, A_2, A_3, ...$ be countable. Then for each n we can list A_n as

$$A_n = \{a_{n,1}, a_{n,2}, a_{n,3}, ...\}.$$

Now list the union by going along diagonals:

$$a_{1,1};\ a_{1,2}, a_{2,1};\ a_{1,3}, a_{2,2}, a_{3,1};\ a_{1,4}, a_{2,3}, a_{3,2}, a_{4,1};\ ...$$

Every element of every A_n appears somewhere in this list, so $\bigcup_{n=1}^{\infty} A_n$ can be listed in a sequence. Hence $\bigcup_{n=1}^{\infty} A_n$ is countable.

(b) Let B_n be the set of all binary strings of length n. Each B_n is finite (there are 2^n such strings), hence countable. Every finite binary string has some length, so

$$B = \{\text{all finite binary strings}\} = \bigcup_{n=0}^{\infty} B_n.$$

By (a), a countable union of countable sets is countable, so B is countable.

(c) Suppose, for contradiction, that the set of irrationals $\mathbb{R} \setminus \mathbb{Q}$ were countable. We already know $\mathbb{Q}$ is countable. Then by part (a),

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

would be a union of two countable sets, hence countable. But $\mathbb{R}$ is uncountable. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

Application — Computability of Functions

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 170–177.*

An important application of the topic of countability to computer science is examining the **computability** of functions. In computer science, a function is **computable** if there is a computer program in some programming language that can find the values of the function. If there is no such program, we say the function is **uncomputable**.

Application problems

1. (a) Show the set of all computer programs in any given computer language is countable.

   Hint: a computer program written in a programming language can be thought of as a string of symbols from a finite alphabet.

   (b) Let T be the set of all functions from $\mathbb{Z}^+$ to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.

   Hint: start by finding an injection between the interval $(0, 1)$ *and a subset of* T*.*

   (c) Hence show that there are uncomputable functions.

Application solutions

1. (a) Given a computer language with a finite alphabet A, we let P be the set of all computer programs in the language. If P is finite, then it is countable and we are done, so assume P is infinite.

   Now we use the fact that we can think of each computer program as a series of strings made using the alphabet A. Consider all strings of length m made from alphabet A, and denote this set by A_m. It is easy to show that there are $|A|^m$ distinct strings of this type, and since A is finite, $|A|^m$ is also finite. Now P is a subset of $\bigcup_{i=1}^{\infty} A_m$. Since the union of a countable number of countable sets is also countable (see Question 3(a) from earlier in this section) it follows that $\bigcup_{i=1}^{\infty} A_m$ is countable and hence P is countable.

   (b) We use the hint and start by defining a function from $(0, 1)$ to T as follows. Recall that every real number in the interval $(0, 1)$ can be written in decimal notation as $0.a_1a_2a_3 \ldots a_n \ldots$ where each a_i is an integer from 0 to 9. Also recall that T is the set of all functions from $\mathbb{Z}^+$ to $\{0, 1, \ldots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

   $$f(0.a_1a_2a_3 \ldots a_n \ldots) = g,$$

   where g is the function in T such that $g(n) = a_n$ for all $n \in \mathbb{Z}^+$.

   So for example, if $f(0.457013) = g$ then g is the function where $g(1) = 4$, $g(2) = 5$, $g(3) = 7$, $g(4) = 0$, $g(5) = 1$, $g(6) = 3$ and $g(n) = 0$ for all $n \geq 7$.

   Now we will prove that this function is one-to-one. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in (0, 1)$. Then for these functions to be equal, they map every integer to the same value. For this to happen, every decimal digit of x_1 must be equal to the same decimal digit of x_2 and so we must have $x_1 = x_2$.

   Now denote the set of all outputs of f as S. Hence $S \subseteq T$. Now if we set the codomain of f to be S, which is the range of f, we have made this function surjective and hence a

bijection. This means that the subset $S \subseteq T$ is in bijection with the interval $(0, 1)$. Since the interval $(0, 1)$ is uncountable, we must have that S is also uncountable and since $S \subseteq T$, T must also be uncountable.

(c) Part (a) showed us that the set of all computer programs in a given language is countable. This means that there are a countable number of computable functions. However part (b) showed us that there is an uncountable number of functions in the set T, so we must have that some functions are uncomputable.

§29 — Relations on Sets

Epp 4th ed. pp. 442–449 · 5th ed. (metric) pp. 487–494. Lecture 23 (week 8).

Problems

1. Define a relation P on $\mathbb{Z}$ as follows: for every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \; P \; n \iff m \text{ and } n \text{ have a common prime factor.}$$

   (a) Is $15 \; P \; 25$?

   (b) Is $22 \; P \; 27$?

   (c) Is $0 \; P \; 5$?

   (d) Is $8 \; P \; 8$?

2. Let $X = \{a, b, c\}$. Define a relation S on the power set $\mathcal{P}(X)$ as follows: for all sets A and B in $\mathcal{P}(X)$,

$$A \; S \; B \iff A \text{ has the same number of elements as } B.$$

   (a) Is $\{a, b\} \; S \; \{b, c\}$?

   (b) Is $\{a\} \; S \; \{a, b\}$?

   (c) Is $\{c\} \; S \; \{b\}$?

3. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ be sets. Let R be the 'divides' relation. That is, for every ordered pair (a, b) in $A \times B$, we have $a \; R \; b$ if and only if $a \mid b$. Draw an arrow diagram (i.e. the directed graph) of this relation.

Solutions

1. (a) **Yes**, since $15 = 3 \cdot 5$ and $25 = 5 \cdot 5$ share the prime factor 5.

   (b) **No**, since $22 = 2 \cdot 11$ and $27 = 3^3$ share no common prime factor.

   (c) **Yes**, since 0 is divisible by every prime; in particular $5 \mid 0$ and $5 \mid 5$, so 0 and 5 have a common prime factor.

   (d) **Yes**, since $8 = 2^3$ and 2 is a prime factor of 8 (so they share the prime factor 2).

2. (a) **Yes**, since $|\{a, b\}| = 2 = |\{b, c\}|$.

   (b) **No**, since $|\{a\}| = 1 \neq 2 = |\{a, b\}|$.

   (c) **Yes**, since $|\{c\}| = 1 = |\{b\}|$.

3. We have $A \times B = \{(3,4), (3,5), (3,6), (4,4), (4,5), (4,6), (5,4), (5,5), (5,6)\}$. The pairs (a, b) satisfying $a \mid b$ are

$$\{(3,6),\ (4,4),\ (5,5)\} \subseteq A \times B.$$

   So the directed graph has an arrow from 3 (in A) to 6 (in B), an arrow from 4 to 4, and an arrow from 5 to 5 — and no other arrows.

§30 — Reflexivity, Symmetry, Transitivity

Epp 4th ed. pp. 449–459 · 5th ed. (metric) pp. 495–505. Lecture 23 (week 8).

Problems

1. Let $X = \{1, 2, 3, 4, 5\}$ and consider the subset $R \subseteq X \times X$ given by

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3), (3,4), (4,5), (5,1)\}.$$

   (a) Draw an arrow diagram for the binary relation R.

   (b) Draw an arrow diagram for the binary relation R^{-1}.

   (c) Draw an arrow diagram for the binary relation $R \cup R^{-1}$.

   (d) Is R symmetric? Is R^{-1} symmetric? Is $R \cup R^{-1}$ symmetric?

   (e) Is R transitive? Is R^{-1} transitive? Is $R \cup R^{-1}$ transitive?

2. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

- $(1, 2) \in R$
- $(2, 3) \in R$
- R is reflexive
- R is transitive

What is the minimum number of arrows required in an arrow diagram for a relation R that satisfies these criteria?

Solutions

1. (a) The arrow diagram for R has the five vertices $1, 2, 3, 4, 5$ drawn around a circle, with a **loop at every vertex** (from the pairs $(1, 1), \ldots, (5, 5)$) together with the directed 5-cycle

$$1 \to 2 \to 3 \to 4 \to 5 \to 1.$$

(b) The arrow diagram for R^{-1} is the same picture with every non-loop arrow reversed: a loop at every vertex, together with the directed 5-cycle

$$1 \to 5 \to 4 \to 3 \to 2 \to 1,$$

that is, $R^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$.

(c) The arrow diagram for $R \cup R^{-1}$ has a loop at every vertex and a **double-headed arrow** between each consecutive pair around the cycle — that is, both $(i, i + 1)$ and $(i + 1, i)$ for the cycle $1, 2, 3, 4, 5, 1$.

(d) R is **not** symmetric because $(1, 2) \in R$ but $(2, 1) \notin R$.

R^{-1} is **not** symmetric because $(2, 1) \in R^{-1}$ but $(1, 2) \notin R^{-1}$.

$R \cup R^{-1}$ **is** symmetric. If $(a, b) \in R \cup R^{-1}$ then $(a, b) \in R$ or $(a, b) \in R^{-1}$, which means $(b, a) \in R^{-1}$ or $(b, a) \in R$, and thus, in either case, $(b, a) \in R \cup R^{-1}$.

(e) R is **not** transitive because $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

R^{-1} is **not** transitive because $(3, 2), (2, 1) \in R^{-1}$ but $(3, 1) \notin R^{-1}$.

$R \cup R^{-1}$ is **not** transitive because $(1, 2), (2, 3) \in R \cup R^{-1}$ but $(1, 3) \notin R \cup R^{-1}$.

2. R is reflexive, so $(1,1),(2,2),(3,3) \in R$ — a loop on each point of the arrow diagram. We are also given $(1,2),(2,3) \in R$, and R is transitive, so $(1,3) \in R$. R is *not* required to be symmetric, so no further arrows are forced.

$$R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$$

So the **minimum number of arrows required is 6**.

§31 — Equivalence Relations

Epp 4th ed. pp. 459–478 · 5th ed. (metric) pp. 505–523. Lecture 24 (week 9).

Problems

1. Define the binary relations α, β and γ on $\mathbb{Z}$ as follows:

$$\begin{aligned} x \,\alpha\, y &\iff x + y \text{ is an even integer,} \\ x \,\beta\, y &\iff x \text{ is a multiple of } y, \\ x \,\gamma\, y &\iff 3 \text{ is a factor of } x^2 - y^2. \end{aligned}$$

   (a) Fill in the table with 'Yes'/'No' to indicate the properties satisfied by each relation.

	α	β	γ
Reflexive			
Symmetric			
Transitive			
Equivalence relation			

   (b) For each equivalence relation, state its equivalence classes.

2. Let $A = \{a,b,c,d,e\}$ be a set and ρ be a binary relation defined by

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

   For instance, $(a,b) \in \rho$ means $a \,\rho\, b$.

   (a) Draw the directed graph representing ρ.

   (b) Is ρ reflexive? Is ρ symmetric? Is ρ transitive?

(c) Is ρ an equivalence relation on A? If so, give its equivalence classes.

(d) What is the smallest subset τ of ρ which forms an equivalence relation on A?

(e) Give the equivalence classes for τ.

3. Consider a positive integer n and any set of strings S. Define a relation R_n on S by the condition $s\ R_n\ t$ if and only if $s = t$ or both s and t have at least n characters and the first n characters are the same. Show that R_n is an equivalence relation.

Solutions

1. (a)

	α	β	γ
Reflexive	Yes	Yes	Yes
Symmetric	Yes	No	Yes
Transitive	Yes	Yes	Yes
Equivalence relation	Yes	No	Yes

(b) The equivalence relations are α and γ.

For α, notice $x\ \alpha\ y \iff x + y$ is even $\iff x$ and y have the same parity. This means the equivalence classes are $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

For γ, notice $x\ \gamma\ y \iff 3 \mid (x^2 - y^2) \iff x^2 \equiv y^2 \pmod 3$. But modulo 3 the only possible square residues are

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 1 \pmod 3.$$

Hence $x^2 \equiv 0 \pmod 3$ exactly when $3 \mid x$, and $x^2 \equiv 1 \pmod 3$ exactly when $3 \nmid x$. Therefore $x\ \gamma\ y$ iff either both x and y are multiples of 3, or neither is. So the equivalence classes are $\{n \in \mathbb{Z} : 3 \mid n\}$ and $\{n \in \mathbb{Z} : 3 \nmid n\}$. Note that another way to write the equivalence classes is $\{3n \mid n \in \mathbb{Z}\}$ and $\{3n + 1,\ 3n + 2 \mid n \in \mathbb{Z}\}$.

2. (a) A digraph for ρ (vertex set $A = \{a, b, c, d, e\}$) has a **loop at every vertex**, double-headed arrows between each pair of $\{a, b, d\}$ — that is between a and b, between a and d, and between b and d — and a double-headed arrow between c and e. There are no arrows between $\{a, b, d\}$ and $\{c, e\}$.

(b) ρ is **reflexive**: we have $(x, x) \in \rho$ for all $x \in A$ (loops on all vertices).

ρ is **symmetric**: whenever $(x, y) \in \rho$, we have $(y, x) \in \rho$ (no single-direction arrow between any two distinct vertices).

ρ is **transitive**: within $\{a, b, d\}$ all relations occur, within $\{c, e\}$ all relations occur, and there are no relations between $\{a, b, d\}$ and $\{c, e\}$. That is, whenever (x, y) and (y, z) are in ρ, then (x, z) is also in ρ (and $x = z$ is possible).

(c) **Yes**, ρ is an equivalence relation. Its equivalence classes are

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

(d) An equivalence relation $\tau \subseteq \rho$ must be reflexive, so $(x, x) \in \tau$ for all $x \in A$. But notice if τ is the relation

$$\tau = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$$

then τ is an equivalence relation. Therefore this is the smallest relation which is an equivalence relation.

(e) The equivalence classes for τ are the singletons:

$$[a] = \{a\},\ [b] = \{b\},\ [c] = \{c\},\ [d] = \{d\},\ [e] = \{e\}.$$

3. Let S be any set of strings and fix $n \in \mathbb{Z}^+$.

   R_n **is reflexive:** for any $s \in S$, since $s = s$, by definition $s\ R_n\ s$.

   R_n **is symmetric:** let $s, t \in S$, and assume $s\ R_n\ t$. If $s = t$ then $t\ R_n\ s$; otherwise both s and t must have at least n characters and, since $s\ R_n\ t$, they must have the same first n characters, so $t\ R_n\ s$.

   R_n **is transitive:** let $s, t, u \in S$ and assume $s\ R_n\ t$ and $t\ R_n\ u$. Since $s\ R_n\ t$ we either have $s = t$, or s and t both have at least n characters and have the same first n characters. Similarly, since $t\ R_n\ u$, either $t = u$, or t and u both have at least n characters and have the same first n characters. Thus either $s = t = u$, or s and u both have at least n characters and they both share the first n characters with t (and hence each other). Thus $s\ R_n\ u$ and so R_n is transitive.

   Since R_n is reflexive, symmetric and transitive it is an equivalence relation. □

Application — Identifiers

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 608–618.*

In the C programming language, an **identifier** is the name of a variable, a function or another type of entity.

Each identifier is a nonempty string of characters where each character is a lowercase or uppercase English letter, a digit, or an underscore.

There is no limit on the number of characters used in the identifier; however, for some compilers for some versions of C, there is a limit on the number of characters checked when two names are compared.

For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. We see that two identifiers will be considered the same if and only if they are related under the relation R_n when $n = 31$ (defined in a previous question).

Application problems

1. Using R_{31} on the set of all possible identifiers, determine the equivalence classes of each of the following identifiers:

   (a) `file_1`

   (b) `Number_of_tropical_storms`

   (c) `Number_of_named_tropical_storms`

   (d) `Number_of_named_tropical_storms_in_the_Atlantic_in_2005`

Application solutions

1. Let I be the set of all possible identifiers (strings over letters, digits and underscores).

   (a) Since `file_1` has length $6 < 31$, its equivalence class is just

   $$[\texttt{file_1}]_{R_{31}} = \{\texttt{file_1}\}.$$

   (b) Since `Number_of_tropical_storms` has length $25 < 31$, its equivalence class is

   $$[\texttt{Number_of_tropical_storms}]_{R_{31}} = \{\texttt{Number_of_tropical_storms}\}.$$

(c) The identifier `Number_of_named_tropical_storms` has length exactly 31, so two identifiers are R_{31}-equivalent to it iff they have at least 31 characters and their first 31 characters equal this string. Hence

$$[\texttt{Number_of_named_tropical_storms}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 31 characters of} \\ t \text{ are } \texttt{Number_of_named_tropical_storms} \end{array} \right\}.$$

(d) The identifier `Number_of_named_tropical_storms_in_the_Atlantic_in_2005` begins with the same first 31 characters `Number_of_named_tropical_storms`, so it has the same R_{31}-equivalence class as in (c):

$$[\texttt{Number_of_named_tropical_storms_in_the_Atlantic_in_2005}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 3} \\ t \text{ are } \texttt{Number_of_name} \end{array} \right.$$

§32 — Partial Order Relations

Epp 4th ed. pp. 498–515 · 5th ed. (metric) pp. 546–563. Lecture 25 (week 9).

Problems

1. Let ρ be a relation on $\mathbb{Z}$ defined by $x \rho y$ if and only if $x^3 - 1 < y^3$.
   (a) Prove ρ is a partial order relation.
   (b) Is ρ a total order?
2. Let S be the set of binary strings of length 6. Define the **weight** of a binary string as the number of ones it contains. (For example, weight(110110) = 4.) Define a relation ρ on S by

   $$s \rho t \text{ if and only if } \text{weight}(s) \leq \text{weight}(t).$$

   (a) Prove that ρ is not an equivalence relation.
   (b) Prove that ρ is not a partial order relation.
3. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:
   - $(2, 3) \in R$
   - $(3, 2) \in R$
   - $(1, 1) \notin R$

- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) To show that ρ is a partial order, we need to show that ρ is reflexive, antisymmetric and transitive.

   Reflexive: let $x \in \mathbb{Z}$. Then $x^3 - 1 < x^3$ and so $x \rho x$, so ρ is reflexive.

   Antisymmetric: suppose $x \rho y$ where $x \neq y$. (We must show that then $y \not\rho x$.) Now $x \rho y$ means that $x^3 - 1 < y^3$. And since $x \neq y$ we must have $x^3 < y^3$ and so $x^3 \leqslant y^3 - 1$. Hence $y^3 - 1 \not< x^3$ and so we do not have $y \rho x$. Therefore ρ is antisymmetric.

   Transitive: suppose that $x \rho y$ and $y \rho z$. Then we know that $x^3 - 1 < y^3$ and $y^3 - 1 < z^3$. So $x^3 - 1 \leqslant y^3 - 1 < z^3$, that is, $x^3 - 1 < z^3$ so that $x \rho z$, which means that ρ is transitive.

   Hence ρ is a partial order. □

   (b) To check whether ρ is a total order, let x and y be any two distinct integers. Then $x^3 \neq y^3$ and so either $x^3 < y^3$ or else $y^3 < x^3$.

   If $x^3 < y^3$ then $x^3 - 1 < y^3$ and so $x \rho y$.

   If $y^3 < x^3$ then $y^3 - 1 < x^3$ and so $y \rho x$.

   So for any integers $x \neq y$, we have either $x \rho y$ or else $y \rho x$. So any two integers are comparable under ρ. Hence ρ **is** a total order.

2. (a) It is **not an equivalence relation** because it is not symmetric. For instance, let $s = 000000$ and $t = 111111$. Then $\text{weight}(s) = 0 \leq 6 = \text{weight}(t)$, so $(s, t) \in \rho$, but $(t, s) \notin \rho$.

   (b) It is **not a partial order** because it is not antisymmetric. For instance, let $s = 100000$ and $t = 010000$. Then $\text{weight}(s) = \text{weight}(t) = 1$, so $s \rho t$ and $t \rho s$, but $s \neq t$.

3. One relation on $\{1, 2, 3\}$ satisfying all conditions is

$$R = \{(1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3, 2)\}.$$

(It contains $(2,3)$ and $(3,2)$; it is transitive; it is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$; it is not antisymmetric since $2 \neq 3$ and $(2,3),(3,2) \in R$; and $(1,1) \notin R$.)

An arrow diagram for this R has vertices $1,2,3$ with: arrows $1 \to 2$ and $1 \to 3$; loops at 2 and at 3; and a double-headed arrow between 2 and 3. There is no loop at vertex 1.

§33 — Definitions and Examples of Groups

No relevant textbook pages. Lecture 26 (week 9).

Problems

1. Show $\mathbb{Z}_9 - \{0\} = \{1,2,3,\ldots,7,8\}$ is not a group under multiplication modulo 9.
2. Let G be the set of all odd integers. Define the binary operation $\star$ on G by

$$x \star y = x + y - 1.$$

   Show that $(G, \star)$ is an abelian group.
3. Show $\mathbb{Z}_9 - \{0,3,6\} = \{1,2,4,5,7,8\}$ is a group under multiplication modulo 9. Is the group abelian?
4. Define the group $H = \mathbb{Z}_5 - \{0\} = \{1,2,3,4\}$ under multiplication modulo 5. Write the Cayley table for H.
5. Define the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ under component-wise addition modulo 2. That is,

$$(a,b) + (c,d) = (a + c \bmod 2,\ b + d \bmod 2).$$

   Write the Cayley table for G.

Solutions

1. It is not a group under multiplication mod 9 because, for example, it is **not closed** ($3 \cdot 3 = 0 \notin \mathbb{Z}_9 - \{0\}$).

2. **Closure:** if x and y are odd, then $x+y$ is even, so $x+y-1$ is odd. Hence $x \star y \in G$.

   Associativity: for $x, y, z \in G$,

$$(x \star y) \star z = (x+y-1)+z-1 = x+y+z-2 = x+(y+z-1)-1 = x \star (y \star z).$$

   Commutativity: for $x, y \in G$,

$$x \star y = x+y-1 = y+x-1 = y \star x.$$

   Identity: we seek $e \in G$ such that $x \star e = x = e \star x$ for all x. Now the requirement $x \star e = x+e-1 = x$ implies that $e = 1$. Note 1 lies in G. Moreover, commutativity implies that $e \star x = x$ as well. Thus the identity is 1.

   Inverses: given $x \in G$, we want $y \in G$ with $x \star y = 1$. This means $x+y-1 = 1$, so $y = 2-x$. Since x is odd, $2-x$ is odd, hence $2-x \in G$. Thus the inverse of x is $x^{-1} = 2-x$.

   Therefore $(G, \star)$ is an abelian group. $\square$

3. **Closure:** if $a, b \in \{1,2,4,5,7,8\}$, then $3 \nmid a$ and $3 \nmid b$, hence $3 \nmid ab$, so $ab \not\equiv 0, 3, 6 \pmod 9$; thus $\{1,2,4,5,7,8\}$ is closed under multiplication modulo 9.

   Associativity and commutativity: normal multiplication between integers is associative and commutative, so multiplication modulo 9 in the set $\{1,2,4,5,7,8\}$ is also associative and commutative. This means the group **is abelian**.

   Identity: $1 \in G$ is the identity because $1 \cdot x \equiv x \pmod 9$.

   Inverse: every element has an inverse. We explicitly calculate the inverses:

$$\begin{aligned}
1^{-1} &= 1 \quad \text{because } 1 \cdot 1 \equiv 1 \pmod 9, \\
2^{-1} &= 5 \quad \text{because } 2 \cdot 5 = 10 \equiv 1 \pmod 9, \\
4^{-1} &= 7 \quad \text{because } 4 \cdot 7 = 28 \equiv 1 \pmod 9, \\
5^{-1} &= 2 \quad \text{because } 5 \cdot 2 = 10 \equiv 1 \pmod 9, \\
7^{-1} &= 4 \quad \text{because } 7 \cdot 4 = 28 \equiv 1 \pmod 9, \\
8^{-1} &= 8 \quad \text{because } 8 \cdot 8 = 64 \equiv 1 \pmod 9.
\end{aligned}$$

4. For $H = \mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ under multiplication mod 5, the Cayley table is:

$\cdot$	1	2	3	4
1	1	2	3	4

$\cdot$	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition mod 2, the Cayley table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(\mathbf{1},\mathbf{0})$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

§34 — Elementary Properties of Groups

No relevant textbook pages. Lecture 27 (week 10).

Problems

1. Let $H = \{3n \mid n \in \mathbb{Z}\}$ be the set of multiples of 3. Prove H is a subgroup of $(\mathbb{Z}, +)$.
2. Fix elements g and h in a group G where e is the group identity. Prove the following statements:
   (a) If $g^{-1} = h$ then $h^{-1} = g$.
   (b) $(g^{-1})^{-1} = g$.
   (c) $(gh)^{-1} = h^{-1}g^{-1}$.
3. Prove $K = \{(0,0),(0,1),(2,0),(2,1)\}$ is a subgroup of $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ where the group operation is componentwise addition:

$$(a,b) + (c,d) = (a + c \pmod 4,\ b + d \pmod 2).$$

4. Consider the group $(\mathbb{Z}_{11} - \{0\}, \cdot)$. Show that this group is cyclic.
   Hint: express every element of $\mathbb{Z}_{11} - \{0\}$ as a power of 2.

Solutions

1. First we note that $H \subseteq \mathbb{Z}$, and $H \neq \emptyset$.

   Closure: if $x, y \in H$ then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}$. Therefore $x + y = 3a + 3b = 3(a + b) \in H$.

   Identity: the identity of $(\mathbb{Z}, +)$ is 0, and since $0 = 3 \cdot 0$, we have $0 \in H$.

   Inverse: in $\mathbb{Z}$, the inverse of x is $-x$. In H, if $x \in H$ then $x = 3a$ for some $a \in \mathbb{Z}$. This means $-x = -3a = 3 \cdot (-a)$, and so $-x \in H$ also.

   Note that we do not need to check associativity for subgroups, since this property is automatically inherited from the parent group $(\mathbb{Z}, +)$. □

2. (a) Suppose $g^{-1} = h$. Now $gh = gg^{-1} = e$ and $hg = g^{-1}g = e$. Thus $h^{-1} = g$.

   (b) By definition, $gg^{-1} = e = g^{-1}g$, so $(g^{-1})^{-1} = g$.

   (c) Notice we have

   $$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = e$$

   and

   $$(h^{-1}g^{-1})(gh) = h^{-1}g^{-1}gh = e.$$

   This means $(gh)^{-1} = h^{-1}g^{-1}$.

3. We draw the Cayley table of $K = \{(0,0), (0,1), (2,0), (2,1)\}$ under componentwise addition in $\mathbb{Z}_4 \times \mathbb{Z}_2$:

$+$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(2,1)$	$(2,0)$
$(\mathbf{2},\mathbf{0})$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(\mathbf{2},\mathbf{1})$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$

   Notice the operation is closed in K and every element of K has an inverse in K. Therefore K is a subgroup. □

4. Note that 2 is a generator of $(\mathbb{Z}_{11} - \{0\}, \cdot)$, so it is cyclic:

   $$1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ 8 = 2^3,\ 5 = 2^4,\ 10 = 2^5,\ 9 = 2^6,\ 7 = 2^7,\ 3 = 2^8,\ 6 = 2^9.$$

§35 — Group Isomorphisms

No relevant textbook pages. No lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36).

This content is optional and will not be assessed. The source document carries no practice problems or solutions for this section.

§36 — Definitions and Examples of Fields

No relevant textbook pages. Lecture 28 (week 10).

Problems

1. (a) Solve $3x + 4 = 2$ in the field $(\mathbb{Z}_5, +, \cdot)$.
   (b) Solve $8x - 9 = 6$ in the field $(\mathbb{Z}_{11}, +, \cdot)$.
   (c) Solve $4(1 - x) = 10$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.
   (d) Solve $16(x - 6) = 15$ in the field $(\mathbb{Z}_{19}, +, \cdot)$.
2. Prove $\mathbb{Z}_{12}$ with addition modulo 12 and multiplication modulo 12 is not a field.
3. Define addition and multiplication on $\mathbb{Q} \times \mathbb{Q}$ by

$$(a, b) + (c, d) = (a + c,\ b + d)$$

   and

$$(a, b) \cdot (c, d) = (ac + 3bd,\ ad + bc)$$

   for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$. Prove that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field.

Solutions

1. (a)

$$\begin{aligned} 3x + 4 &= 2 \\ \rightarrow 3x &= -2 \end{aligned}$$

Now, since $3 \times 2 = 6 \equiv 1 \pmod 5$, 2 is the multiplicative inverse of 3, and so we multiply both sides by 2 and obtain $x = -4$. That is, $x = 1$.

Check: $3 \cdot 1 + 4 = 7 \equiv 2 \pmod 5$.

(b)

$$\begin{aligned} 8x - 9 &= 6 \\ \rightarrow 8x &= 15 = 4 \end{aligned}$$

Now, since $8 \times 7 = 56 \equiv 1 \pmod{11}$, 7 is the multiplicative inverse of 8, and so we multiply both sides by 7 and obtain $x = 28$. That is, $x = 6$.

Check: $8 \cdot 6 - 9 = 39 \equiv 6 \pmod{11}$.

(c) Since $4 \times 10 = 40 \equiv 1 \pmod{13}$, 10 is the multiplicative inverse of 4, and so we multiply both sides by 10 and obtain $1 - x = 100 = 9$. That is, $x = 1 - 9 = 14 - 9 = 5$.

Check: $4(1 - 5) = -16 \equiv 10 \pmod{13}$.

(d) Since $16 \times 6 = 96 \equiv 1 \pmod{19}$, 6 is the multiplicative inverse of 16, and so we multiply both sides by 6 and obtain $x - 6 = 90 = 14$. That is, $x = 20 = 1$.

Check: $16(1 - 6) = -80 \equiv 15 \pmod{19}$.

2. $\mathbb{Z}_{12}$ is not a field because 2 has no multiplicative inverse modulo 12. Indeed $2 \cdot k \equiv 1 \pmod{12}$ has no solution since $2k$ is always even.

3. We show that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field in three steps.

Step 1 — $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Closure: for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Q} \times \mathbb{Q}$.

Associative: for all $(a, b), (c, d), (e, f) \in \mathbb{Q} \times \mathbb{Q}$ we have $\big((a, b) + (c, d)\big) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) = (a, b) + (c + e, d + f) = (a, b) + \big((c, d) + (e, f)\big)$.

Identity: for all $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0) + (a, b)$.

Inverses: for all $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a,b) + (-a,-b) = (a-a, b-b) = (0,0)$ and $(-a,-b) + (a,b) = (-a+a, -b+b) = (0,0)$. So $(-a,-b)$ is the inverse of (a,b).

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b)$.

Thus $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Step 2 — $((\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\},\ \cdot)$ is an abelian group.

Closure: for all $(a,b),(c,d) \in (\mathbb{Q}\times\mathbb{Q}) - \{(0,0)\}$, we have $(a,b)\cdot(c,d) = (ac+3bd, ad+bc) \in \mathbb{Q} \times \mathbb{Q}$. So we only need to show that $(ac+3bd, ad+bc) \neq (0,0)$. For a contradiction, suppose $(ac+3bd, ad+bc) = (0,0)$. That is, $ac+3bd = 0$ and $ad+bc = 0$. Multiplying the first equation by d and the second by c we obtain $acd + 3bd^2 = 0$ and $acd + bc^2 = 0$, from which it follows that $3bd^2 = bc^2$.

Now, if $b = 0$, then $ac = 0$, $ad = 0$ and $a \neq 0$, and so $c = d = 0$; a contradiction. Thus $b \neq 0$ and we have $3d^2 = c^2$. This is a contradiction because if $d = 0$, then $c \neq 0$ and the equation does not hold, and if $d \neq 0$, then we have $3 = \frac{c^2}{d^2}$, which implies $\sqrt{3} = \frac{c}{d}$ is rational. Thus $(ac+3bd, ad+bc) \neq (0,0)$ and we have closure.

Associative: for all $(a,b),(c,d),(e,f) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have

$$\begin{aligned}(a,b)\cdot\big((c,d)\cdot(e,f)\big) &= (a,b)\cdot(ce+3df,\ cf+de)\\ &= (a(ce+3df)+3b(cf+de),\ a(cf+de)+b(ce+3df))\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf)\end{aligned}$$

and

$$\begin{aligned}\big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac+3bd,\ ad+bc)\cdot(e,f)\\ &= \big((ac+3bd)e+3(ad+bc)f,\ (ac+3bd)f+(ad+bc)e\big)\\ &= (ace+3bde+3adf+3bcf,\ acf+3bdf+ade+bce)\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf).\end{aligned}$$

Identity: for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have $(a,b)\cdot(1,0) = (a,b)$ and $(1,0)\cdot(a,b) = (a,b)$, so $(1,0)$ is a multiplicative identity.

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have

$$(a,b)\cdot(c,d) = (ac+3bd,\ ad+bc) = (ca+3db,\ cb+da) = (c,d)\cdot(a,b).$$

Inverses: we check that for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2-3b^2},\ \frac{-b}{a^2-3b^2}\right).$$

First, note that $a^2-3b^2 \neq 0$, because $a^2-3b^2=0$ implies either $(a,b)=(0,0)$ or $\sqrt{3}=\frac{a}{b}$, both of which are contradictions (the second because $\sqrt{3}$ is not rational). Thus $(a,b)^{-1} \in (\mathbb{Q}\times\mathbb{Q})-\{(0,0)\}$, and notice

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2-3b^2},\frac{-b}{a^2-3b^2}\right) &= \left(a\cdot\frac{a}{a^2-3b^2}+3b\cdot\frac{-b}{a^2-3b^2},\ a\cdot\frac{-b}{a^2-3b^2}+b\cdot\frac{a}{a^2-3b^2}\right)\\ &= \left(\frac{a^2-3b^2}{a^2-3b^2},\ \frac{-ab+ab}{a^2-3b^2}\right)\\ &= (1,0).\end{aligned}$$

So every nonzero element has an inverse. Thus $((\mathbb{Q}\times\mathbb{Q})-\{(0,0)\},\cdot)$ is an abelian group.

Step 3 — the distributive laws. For all $(a,b),(c,d),(e,f)\in\mathbb{Q}\times\mathbb{Q}$ we have

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,\ d+f)\\ &= (a(c+e)+3b(d+f),\ a(d+f)+b(c+e))\\ &= ((ac+3bd)+(ae+3bf),\ (ad+bc)+(af+be))\\ &= (ac+3bd,\ ad+bc)+(ae+3bf,\ af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)\end{aligned}$$

and (since we have already shown that multiplication and addition are commutative)

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f) &= (e,f)\cdot((a,b)+(c,d))\\ &= (e,f)\cdot(a,b)+(e,f)\cdot(c,d) \quad \text{(by the first distributive law)}\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f).\end{aligned}$$

Thus $(\mathbb{Q}\times\mathbb{Q},+,\cdot)$ is a field. □

§37 — Introduction to Counting

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 29 (week 11).

Problems

1. The UQ drama club is auditioning for its annual production of *Romeo and Juliet*. Six people are auditioning for the role of Romeo, and eight other people are auditioning for the role of Juliet. In how many ways can the director cast the lead couple?
2. There are eleven questions on the final exam, but you decide — based on your successful grade for your in-semester exam — that you will only do five of them. How many combinations of questions are there which you could complete?
3. (a) How many permutations of $\{1, 2, \dots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \dots, 15\}$ contain exactly two numbers from $\{1, 2, 3, 4\}$?

Solutions

1. There are 6 choices for Romeo and 8 choices for Juliet, so $6 \cdot 8 = 48$ ways.
2. Since the order in which you do the 5 questions does not matter, there are $\binom{11}{5} = 462$ combinations of questions.
3. (a) There are 8 odd numbers in the set $\{1, \dots, 15\}$. Choose the first entry in 8 ways, then permute the remaining 14 numbers, so $8 \cdot 14!$ permutations.

   (b) We choose exactly 2 numbers from the set $\{1, 2, 3, 4\}$ and exactly 3 numbers from the remaining 11 numbers, so the number of subsets is

$$\binom{4}{2}\binom{11}{3}.$$

Application — Runtime

Not assessable for MATH1061. Taken from S. Epp, Discrete Mathematics with Applications, *5th edition, pages 787–799.*

In many algorithms, the runtime is well approximated by counting how many times the basic instructions are executed.

For programs with nested `for`-loops and no early exits, the total number of executions of the inner loop body equals the number of choices of the outer-loop index multiplied by the number of choices of the inner-loop index.

Concretely, if i runs through M values and, for each fixed i, the variable j runs through N values, then the inner loop body is executed exactly MN times.

Application problems

1. The following algorithms are written in pseudo-code and contain nested loops. For each algorithm, count the total number of iterations of the inner loop that the algorithm will run.

   (a)

```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (b)

```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (c) (Fix integers $a, b, c, d \in \mathbb{Z}^+$ with $a \leq b$ and $c \leq d$.)

```
for i := a to b
    for j := c to d
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

Application solutions

1. (a) $i = 1, \ldots, 30$ gives 30 iterations and $j = 1, \ldots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

   (b) $i = 5, \ldots, 50$ gives $50 - 5 + 1 = 46$ iterations and $j = 10, \ldots, 20$ gives $20 - 10 + 1 = 11$ iterations, so the inner loop runs $46 \cdot 11 = 506$ times.

   (c) $i = a, \ldots, b$ gives $b - a + 1$ iterations and $j = c, \ldots, d$ gives $d - c + 1$ iterations, so the inner loop runs $(b - a + 1)(d - c + 1)$ times.

§38 — Counting Selections

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 30 (week 11).

Problems

1. (a) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY?

   (b) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with R and end with P?

   (c) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with I and end with Y?

   (d) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that have all four Os next to each other?

2. (a) How many distinct arrangements can be made of the letters of the word WOOLLOONGABBA?

   (b) How many distinct arrangements are there of the letters of the word WOOLLOONGABBA such that **exactly one** of the following is true?

   - The two As are not next to each other.
   - The two Bs are not next to each other.
   - The two Ls are not next to each other.

3. (a) How many one-to-one (injective) functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

   (b) How many onto (surjective) functions are there from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$?

Solutions

1. (a) There are 13 letters in INDOOROOPILLY, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!} = 64\,864\,800.$$

   (b) Fix R in the first position and P in the last position. There are 11 letters remaining, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!\,2!} = 415\,800.$$

(c) Fix I in the first position and Y in the last position. There are 11 letters remaining, with four O's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!} = 831\,600.$$

(d) Treat the four O's as one 'letter'. There are 10 'letters' with two I's, two L's, and the remaining 'letters' appearing once each. Therefore the number of distinct arrangements is

$$\frac{10!}{2!\,2!} = 907\,200.$$

2. (a) There are 13 letters in WOOLLOONGABBA, with four O's, two L's, two A's, two B's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!\,2!} = 32\,432\,400.$$

(b) We want exactly one of the pairs AA, BB, LL to be non-adjacent. That is, there are three cases to consider:

- **Case 1:** the two A's are not adjacent but BB and LL are adjacent.
- **Case 2:** the two B's are not adjacent but AA and LL are adjacent.
- **Case 3:** the two L's are not adjacent but AA and BB are adjacent.

Note that the number of ways Case 1 can occur is exactly the same as the number of ways Case 2 can occur (and similarly for Case 3).

To count the number of ways Case 1 can occur, we first count arrangements with BB adjacent and LL adjacent. Treat BB as one 'letter' and LL as one 'letter'. Then there are 11 'letters' (W, O, O, LL, O, O, N, G, A, BB, A) to arrange, with four O's, two A's, and the remaining 'letters' appearing once each. Therefore the number of such arrangements is

$$\frac{11!}{4!\,2!}.$$

In order to determine the number of these for which the two A's are not adjacent, we take this total and subtract those where AA is also adjacent. For this, treat AA, BB, and LL as 'letters'. Then there are 10 'letters' to arrange, with four O's and the remaining 'letters' appearing once each. Therefore the number of arrangements with AA adjacent and BB adjacent and LL adjacent is

$$\frac{10!}{4!}.$$

Hence, the number of ways that Case 1 can occur is

$$\frac{11!}{4!\,2!} - \frac{10!}{4!}.$$

Case 2 and Case 3 have exactly the same number of occurrences as Case 1. Also note that the three cases are mutually exclusive (you cannot have both Case 1 and Case 2 occurring at the same time, for example).

So the number of arrangements of the word WOOLLOONGABBA for which exactly one of the three cases occurs is

$$3\left(\frac{11!}{4!\,2!} - \frac{10!}{4!}\right).$$

3. (a) An injective function $f : \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ is determined by choosing distinct images for a, b, c. The number of choices is

$$5 \cdot 4 \cdot 3 = {}^5P_3 = 60.$$

(b) The number of surjective functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ is the total number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ minus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ which are not surjective. The former number is 3^5. A function which is not surjective must have image of size 1 or 2.

- In the first case, there are 3 such functions (one for each of the three choices for the image).
- In the latter case, first choose which 2 elements of $\{a, b, c\}$ will be in the image. There are $\binom{3}{2}$ such choices. For this fixed two-element image, the number of functions with this image is

$$2^5 - 2,$$

since there are 2^5 total functions from a 5-element set to a 2-element set, and we subtract the 2 constant ones (which fall into the first case, having image of size 1). Thus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ with an image of size 2 is

$$\binom{3}{2}(2^5 - 2) = 3 \cdot 30 = 90.$$

This means there are 93 functions which are not surjective, so the number of surjective functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ is

$$3^5 - 93 = 150.$$

§39 — Introduction to Probability

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 31 (week 11).

Problems

1. To form a committee, five people are to be chosen from a group of ten people.
   (a) How many different committees of five can be chosen?
   (b) Amongst the ten people, we have Alice, Bob, Eve and Oscar. Alice and Bob are extremely talkative during meetings, and so at most one of these two can be chosen. Eve and Oscar are inseparable, and so a committee must either contain both of them or neither of them. With these constraints, how many different five-person committees can be formed?
   (c) What is the probability that none of Alice, Bob, Eve and Oscar are on a committee, given that a random committee of five is chosen subject to the constraints in part (b)?
2. (a) How many positive two-digit integers are multiples of 3?
   (b) What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
   (c) What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

Solutions

1. (a) Number of different committees of five is

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252.$$

   (b) Let A, B be Alice and Bob, and let E, O be Eve and Oscar. There are 6 other people. We split into cases.

   Case 1: the committee contains both E and O. Then we choose 3 more people from the remaining 8 with the restriction that we cannot choose both A and B. There are $\binom{8}{3}$ ways to choose 3 more people from the remaining 8 to be on the committee; of these, there are $\binom{6}{1}$ ways in which both A and B are chosen (such a committee must have E, O, A, B so there is only one more person to choose from the remaining 6 people). Thus the number of committees for this case is

$$\binom{8}{3} - \binom{6}{1} = 56 - 6 = 50.$$

   Case 2: the committee contains neither E nor O. Then we choose 5 people from the remaining 8, again not allowing both A and B. There are $\binom{8}{5}$ ways to choose 5 people from the remaining 8 people to be on the committee; of these, there are $\binom{6}{3}$ ways in which both A and B are chosen. Thus the number of committees for this case is

$$\binom{8}{5} - \binom{6}{3} = 56 - 20 = 36.$$

   Hence the total number is $50 + 36 = 86$.

   (c) To have none of Alice, Bob, Eve, or Oscar on the committee, we must choose all 5 members from the other 6 people, which can be done in $\binom{6}{5} = 6$ ways. Therefore the probability is

$$\frac{6}{86} = 0.069767\ldots$$

2. (a) The positive two-digit multiples of 3 occur as every third number from 12 to 99, so there are

$$\frac{99 - 12}{3} + 1 = 30$$

such numbers.

(b) There are 90 positive two-digit integers (9 choices for the first digit and 10 choices for the second digit). Thus, by part (a), the probability that a randomly selected positive two-digit number is a multiple of 3 is

$$\frac{30}{90} = \frac{1}{3}.$$

(c) The positive two-digit multiples of 4 occur as every fourth number from 12 to 96, so there are

$$\frac{96-12}{4} + 1 = 22$$

such numbers. Hence the probability that a randomly selected positive two-digit number is a multiple of 4 is

$$\frac{22}{90} = \frac{11}{45}.$$

§40 — Binomial Coefficients

Epp 4th ed. pp. 565–591 · 5th ed. (metric) pp. 617–641. Lecture 31 (week 11).

Problems

1. What is the coefficient of x^4 in $(2+3x)^7$?
2. (a) What is the coefficient of x^{12} in $(3-x^3)^6$?
   (b) What is the coefficient of x^8 in $(3-x^3)^6$?
3. What is the coefficient of x^2 in the expansion of $(3-x)^6$?
4. What is the coefficient of x^5 in the expansion of $(2x+1)^{20}$?
5. What is the coefficient of x^5 in the expansion of $\left(3x^2 - \dfrac{2}{x}\right)^7$?

Solutions

1. By the binomial theorem,

$$(2+3x)^7 = \sum_{k=0}^{7} \binom{7}{k} 2^{7-k}(3x)^k.$$

The term x^4 appears only when $k=4$. This term is $\binom{7}{4}2^3(3x)^4$. Therefore the coefficient of x^4 is

$$\binom{7}{4}2^3 3^4 = 35 \times 8 \times 81 = 22\,680.$$

2. By the binomial theorem,

$$(3-x^3)^6 = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-x^3)^k = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-1)^k x^{3k}.$$

(a) The term involving x^{12} is $\binom{6}{4}3^2(-1)^4 x^{3\cdot 4}$, so the coefficient of x^{12} is

$$15 \times 9 \times (-1)^4 = 135.$$

(b) Every power of x that appears is a multiple of 3. Since 8 is not a multiple of 3, there is no x^8 term, so the coefficient of x^8 is $\mathbf{0}$.

3. By the binomial theorem,

$$(3-x)^6 = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-x)^i = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-1)^i x^i.$$

The term x^2 appears only when $i=2$, so the coefficient of x^2 is

$$\binom{6}{2}3^{6-2}(-1)^2 = \binom{6}{2}3^4 = 1215.$$

4. By the binomial theorem,

$$(2x+1)^{20} = \sum_{k=0}^{20} \binom{20}{k} (2x)^{20-k}(1)^k.$$

The term x^5 appears only when $k = 15$, where the term is $\binom{20}{15}(2x)^5$, so the coefficient of x^5 is

$$\binom{20}{5} 2^5 = 496\,128.$$

5. By the binomial theorem,

$$\left(3x^2 - \frac{2}{x}\right)^7 = \sum_{i=0}^{7} \binom{7}{i} (3x^2)^{7-i} \left(-\frac{2}{x}\right)^i = \sum_{i=0}^{7} \binom{7}{i} 3^{7-i}(-2)^i x^{14-3i}.$$

The term x^5 appears only when $14 - 3i = 5$, i.e. $i = 3$. Therefore the coefficient of x^5 is

$$\binom{7}{3} 3^4(-2)^3 = -22\,680.$$

§41 — Inclusion Exclusion

Epp 4th ed. pp. 545–549 · 5th ed. (metric) pp. 595–599. Lecture 32 (week 12).

Problems

1. Out of 100 people surveyed, 40 people like apples, 50 like bananas and 40 like cherries. 15 like apples and bananas, 16 like bananas and cherries, 17 like cherries and apples and 10 people like all three. How many people do not like any of the three fruits?
2. How many integers between 1 and 600 inclusive are coprime with 15? That is, how many integers n satisfy $1 \leq n \leq 600$ and $\gcd(n, 15) = 1$?
3. Seven friends, named Alice, Bob, Charlie, Delia, Edward, Fred and George, stand in a line for a photograph. How many different arrangements are there of the seven friends standing in a line such that Alice is not next to Charlie and Bob is not next to Delia?

Solutions

1. Let A be the set of people who like apples, B the set of people who like bananas, and C the set of people who like cherries. We are given

$$|A| = 40,\ |B| = 50,\ |C| = 40, \quad |A \cap B| = 15,\ |B \cap C| = 16,\ |C \cap A| = 17, \quad |A \cap B \cap C| = 10.$$

   By inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \\ &= 40 + 50 + 40 - 15 - 17 - 16 + 10 \\ &= 92. \end{aligned}$$

   Hence the number of people who do not like any of the three fruits is

$$100 - |A \cup B \cup C| = 100 - 92 = 8.$$

2. Let $U = \{1, 2, \ldots, 600\}$. Define

$$A = \{n \in U : 3 \mid n\}, \qquad B = \{n \in U : 5 \mid n\}.$$

   Then n is not coprime to 15 if and only if $n \in A \cup B$. We have

$$|A| = \frac{600}{3} = 200, \qquad |B| = \frac{600}{5} = 120, \qquad |A \cap B| = \frac{600}{15} = 40.$$

   By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 200 + 120 - 40 = 280.$$

   Therefore the number of n with $\gcd(n, 15) = 1$ is

$$|U| - |A \cup B| = 600 - 280 = 320.$$

3. Let U be the set of all linear arrangements of the 7 friends, so $|U| = 7!$. Define

$$A = \{\text{arrangements in which Alice is next to Charlie}\},$$
$$B = \{\text{arrangements in which Bob is next to Delia}\}.$$

We want to count the number of arrangements in U which are neither in A nor in B. The required number is $|U \setminus (A \cup B)| = |U| - |A \cup B|$.

To count $|A|$, treat {Alice, Charlie} as a single block. There are 6! ways to arrange the 6 "objects", and for each of these there are 2 ways to order Alice and Charlie within their block (either Alice or Charlie to the left). Hence

$$|A| = 2 \cdot 6!.$$

Similarly, $|B| = 2 \cdot 6!$.

To count $|A \cap B|$, treat both pairs {Alice, Charlie} and {Bob, Delia} as two single blocks. There are 5! ways to arrange the 5 objects (two blocks plus the other three people), and for each of these there are $2 \cdot 2$ internal orders of the two blocks. Hence

$$|A \cap B| = 4 \cdot 5!.$$

By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!.$$

Therefore

$$|U \setminus (A \cup B)| = 7! - (2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!) = 2640.$$

§42 — The Pigeonhole Principle

Epp 4th ed. pp. 554–565 · 5th ed. (metric) pp. 604–616. Lecture 33 (week 12).

Problems

1. (a) Explain why, in a group of 50 people, at least five people were born in the same month.

   (b) How many people do you need to ensure that at least seven people were born in the same month?

2. Show that, if we select six distinct integers from the set $\{1, 2, \ldots, 10\}$, two of these must add to give 11.

3. A computer network consists of six computers. Each computer is directly connected to zero or more of the other computers. Show that there are at least two computers in the network that are directly connected to the same number of other computers.

4. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

5. Let $S = \{1, 2, \ldots, 100\}$. What is the minimum number of integers you must pick from S to be sure that at least one pair has a difference which is divisible by 3?

Solutions

1. (a) There are 12 months (pigeonholes) and 50 people (pigeons). If each month had at most 4 birthdays, then there would be at most $12 \cdot 4 = 48$ people. Since $50 > 48$, by the pigeonhole principle some month must contain at least 5 people.

   (b) To guarantee at least 7 people are born in the same month, note that if each month had at most 6 birthdays, then there could be at most $12 \cdot 6 = 72$ people. Therefore with **73** people, by the pigeonhole principle some month has at least 7 people. Moreover, 72 people is not enough (take 6 born in each month), so the minimum is 73.

2. Partition $A = \{1, 2, \ldots, 10\}$ into the 5 pairs

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\},\ \{5, 6\},$$

   each summing to 11. In order for a selection of distinct integers from the set A to **not** have two that add to give 11, at most one integer can be chosen from each of the subsets. Choosing 6 distinct integers from A forces us to select two numbers from the same pair (there are 5 pairs but 6 choices), by the pigeonhole principle. Those two numbers then add to 11.

3. For each computer, let its **degree** be the number of other computers it is directly connected to. With 6 computers, each degree is an integer in $\{0, 1, 2, 3, 4, 5\}$. It is impossible to have both a computer of degree 0 and a computer of degree 5 (if one is connected to everyone, then none has degree 0). Hence the degrees must all lie in one of the two 5-element sets

$$\{0, 1, 2, 3, 4\} \quad \text{or} \quad \{1, 2, 3, 4, 5\}.$$

So, in either case, there are only 5 possible degree values available for 6 computers. By the pigeonhole principle, at least two computers have the same degree, i.e. are connected to the same number of other computers.

4. Let g_i be the total number of games played in the first i days, for $i = 1, 2, \ldots, 30$. Then

$$1 \leq g_1 < g_2 < \cdots < g_{30} \leq 45$$

because at least one game is played each day. Consider also the 30 numbers

$$g_1 + 14,\ g_2 + 14,\ \ldots,\ g_{30} + 14,$$

which satisfy $15 \leq g_1 + 14 < \cdots < g_{30} + 14 \leq 59$. Thus we have 60 integers

$$g_1, \ldots, g_{30},\ g_1 + 14, \ldots, g_{30} + 14$$

all lying in the set $\{1, 2, \ldots, 59\}$ of size 59. By the pigeonhole principle, two of these 60 integers are equal. Since the g_i are strictly increasing, no equality can occur among the g_i themselves, and likewise no equality can occur among the $g_i + 14$ themselves. Therefore we must have

$$g_j = g_i + 14$$

for some $i, j \in \{1, \ldots, 30\}$. Then the number of games played from day $i + 1$ through day j is

$$g_j - g_i = 14,$$

so there is a period of consecutive days during which exactly 14 games are played.

5. First, we note that two integers have a difference that is divisible by 3 if and only if they are congruent modulo 3 (have the same remainder when divided by 3). Now, the set S can be partitioned into three sets based on their congruence class modulo 3. By the pigeonhole principle, if we select **4** numbers from S, at least two of them must belong to the same congruence class. These two will have difference that is divisible by 3. Note that 4 is the minimum number of selections that guarantees this, since it is possible to select 3 numbers where no two of them have difference divisible by 3 (select one from each congruence class).

§43 — Introduction to Graph Theory

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 33 (week 12).

Problems

1. For each of the following, state whether or not there exists a simple graph with the stated number of vertices and degrees. Draw the graph, or explain why one does not exist.
   (a) Five vertices with degrees 3, 3, 2, 2, 2.
   (b) Seven vertices with degrees 4, 2, 3, 1, 1, 1, 1.
   (c) Five vertices with degrees 5, 4, 3, 1, 1.
2. A graph has 10 edges and 6 vertices. Five of the vertices have degree 3. What is the degree of the remaining vertex?
3. Let n be a positive integer and let K_n be the complete graph with n vertices. How many edges does K_n have?
4. A graph has 27 edges and every vertex has degree 2, 3 or 4. If there are 7 vertices that have degree 4 and 4 vertices that have degree 3, then how many vertices of degree 2 are there?

Solutions

1. (a) **Yes**, such a simple graph exists. One drawing has vertices a, b, c, d, e and the six edges

$$ab, \quad ac, \quad ad, \quad bc, \quad be, \quad de,$$

giving $\deg(a) = 3$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 2$, $\deg(e) = 2$ as required.

   (b) **No** such graph exists. If the degrees are 4, 2, 3, 1, 1, 1, 1, then the sum of degrees is

$$4 + 2 + 3 + 1 + 1 + 1 + 1 = 13,$$

which is odd. Remember (by the Handshake Theorem) that the sum of the degrees in any graph equals twice the number of edges, and so is always even. So such a graph cannot exist.

(c) **No** such graph exists. In a simple graph on 5 vertices, the largest possible degree is 4, but the sequence contains a vertex of degree 5, which is impossible. So there is no such simple graph.

2. Since the graph has 10 edges, the sum of all the degrees is $2 \cdot 10 = 20$. If five vertices have degree 3, the sum of their degrees is $5 \cdot 3 = 15$, so the remaining vertex has degree

$$20 - 15 = 5.$$

3. In K_n, an edge is determined by choosing 2 distinct vertices, so the number of edges is

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

4. Let x be the number of vertices of degree 2. Since the graph has 27 edges, the sum of degrees is $2 \cdot 27 = 54$. Given that there are seven vertices of degree 4 and four vertices of degree 3, and all other vertices have degree 2, we have

$$2x + 4 \cdot 7 + 3 \cdot 4 = 54.$$

This means $x = 7$.

§44 — Walks, Trails and Circuits

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 34 (week 12).

Problems

1. Let G and H be the graphs below.

   G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is drawn with a **loop at** v_2, a **loop at** v_5, and **two parallel edges between** v_1 **and** v_2. Its degree sequence is

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   so G is connected with 10 edges.

   H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is a simple connected graph drawn as the 4-cycle $v_1v_2v_3v_4v_1$ with a single pendant edge v_3v_5, giving degrees

   $$\deg(v_1) = 2, \quad \deg(v_2) = 2, \quad \deg(v_3) = 3, \quad \deg(v_4) = 2, \quad \deg(v_5) = 1.$$

   For each of the following statements, explain why it is true or false.

   (a) G is a simple graph.

   (b) The sum of the degrees of the vertices of G is 18.

   (c) G contains an Euler circuit.

   (d) H contains an Euler trail.

2. Does the following graph contain an Euler circuit? (The graph shown is connected and has exactly two vertices of degree 3.)

3. Let G be a simple, connected, Eulerian graph with eight vertices and let e be the number of edges in G. Prove that $8 \leq e \leq 24$.

Solutions

1. (a) This statement is **false**. The graph G has loops (at v_2 and v_5) and it also has multiple edges between v_1 and v_2, so G is not simple.

   (b) This statement is **false**. A loop contributes 2 to the degree, so we have

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   and thus the sum of the degrees is $4 + 6 + 4 + 2 + 4 = 20 \neq 18$.

   (c) This statement is **true**. The graph G is connected and every vertex has even degree (as computed above), so G contains an Euler circuit.

(d) This statement is **true**. In H, the degrees are

$$\deg(v_1) = 2,\ \deg(v_2) = 2,\ \deg(v_4) = 2,\ \deg(v_3) = 3,\ \deg(v_5) = 1,$$

so exactly two vertices have odd degree (namely v_3 and v_5). Therefore H has an Euler trail (starting at one of v_3, v_5 and ending at the other).

2. **No.** The graph is connected, but has two vertices of degree 3, so not all vertices have even degree. Hence there is no Euler circuit.

3. Since G is connected and Eulerian, every vertex has even degree, and (because G is simple and connected with 8 vertices) each vertex has degree at least 2. Hence

$$2e = \sum_{v} \deg(v) \geq 8 \cdot 2 = 16,$$

so $e \geq 8$. Moreover, in a simple graph on 8 vertices we have $\deg(v) \leq 7$, and because G is Eulerian all degrees are even, so in fact $\deg(v) \leq 6$ for every vertex. Therefore

$$2e = \sum_{v} \deg(v) \leq 8 \cdot 6 = 48,$$

so $e \leq 24$. Hence $8 \leq e \leq 24$. □

§45 — Matrix Representations of Graphs

Epp 4th ed. pp. 661–675 · 5th ed. (metric) pp. 698–712. Lecture 35 (week 13).

Problems

1. Let G be the graph with vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{a, b, c, d, e, f\}$, where the edges are

edge	endpoints
a	$v_1 v_2$
b	$v_2 v_3$
c	$v_2 v_3$ (parallel to b)
d	$v_3 v_4$
e	$v_2 v_4$
f	loop at v_4

(a) Write down an adjacency matrix for G. Make sure you clearly label the rows and columns of your matrix.

(b) Write down an incidence matrix for G. Make sure you clearly label the rows and columns of your matrix.

(c) Does G have an Euler circuit? If yes, write it out as a sequence of vertices and edges. If not, determine the fewest number of edges that would need to be added to G to create a new graph that does have an Euler circuit.

2. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(a) Draw the graph G.

(b) Explain whether or not G has an Euler circuit or an Euler trail.

3. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Explain whether or not G is Eulerian.

Solutions

1. (a) The labelled adjacency matrix for G is

	v_1	v_2	v_3	v_4
$\mathbf{v_1}$	0	1	0	0
$\mathbf{v_2}$	1	0	2	1
$\mathbf{v_3}$	0	2	0	1
$\mathbf{v_4}$	0	1	1	1

(where the entry 1 on the diagonal at v_4 records the single loop at v_4).

(b) The labelled incidence matrix for G is

	a	b	c	d	e	f
$\mathbf{v_1}$	1	0	0	0	0	0
$\mathbf{v_2}$	1	1	1	0	1	0
$\mathbf{v_3}$	0	1	1	1	0	0
$\mathbf{v_4}$	0	0	0	1	1	2

(where the entry 2 in the bottom right indicates the loop that is incident twice with v_4).

(c) The degrees are

$$\deg(v_1) = 1, \quad \deg(v_2) = 4, \quad \deg(v_3) = 3, \quad \deg(v_4) = 4,$$

so G does **not** have an Euler circuit (since v_1 and v_3 have odd degree).

The fewest edges to add to make all degrees even is **1**; for example, adding an edge g between vertices v_1 and v_3 creates a new connected graph in which all of the vertices have even degree.

An example of an Euler circuit in the new graph is

$$v_1,\ a,\ v_2,\ b,\ v_3,\ d,\ v_4,\ f,\ v_4,\ e,\ v_2,\ c,\ v_3,\ g,\ v_1.$$

2. (a) Reading the matrix off (with vertices $v_1, \ldots, v_5$ in matrix order), G has the edges

- v_1v_2 — a single edge,
- v_1v_5 — **three** parallel edges,
- v_2v_3 — **two** parallel edges,
- v_3v_4 — a single edge,
- v_3v_5 — a single edge,
- v_4v_5 — a single edge.

(b) The degrees are

$$\deg(v_1) = 4,\ \deg(v_2) = 3,\ \deg(v_3) = 4,\ \deg(v_4) = 2,\ \deg(v_5) = 5,$$

so there is **no Euler circuit** (since v_2 and v_5 have odd degree), but there **is an Euler trail** (exactly two odd-degree vertices) from v_2 to v_5.

3. Let the vertices be $v_1, v_2, v_3, v_4, v_5, v_6$ in the order of the matrix. Reading the matrix off, G has edges

$$v_1v_2, \quad v_1v_4, \quad v_2v_4, \quad v_3v_5, \quad v_3v_6, \quad v_5v_6,$$

that is, two disjoint triangles: one on $\{v_1, v_2, v_4\}$ and one on $\{v_3, v_5, v_6\}$.

The graph is **not connected** (e.g. there is no walk from vertex v_1 to vertex v_3). Hence G is not Eulerian.

(Errata note: the source document's solution to 1(b) was corrected on 11 August 2026 — the note in brackets had previously copied the note from 1(a). The corrected note is the one given above.)

§46 — Trees

Epp 4th ed. pp. 683–701 · 5th ed. (metric) pp. 720–742. Lecture 36 (week 13).

Problems

1. A tree has 11 vertices, of which exactly four vertices have degree 1 and exactly one vertex has degree 4. Determine the degrees of the remaining six vertices.
2. Let T be a tree with p vertices, where $p \geq 11$. Suppose T has precisely six vertices of degree 1 and precisely four vertices of degree 3. Determine the degree of each of the remaining $p - 10$ vertices of T.
3. Let T be a tree on 12 vertices. Suppose T has exactly three vertices of degree 3 and each of the remaining vertices has degree 1 or 5. Using theorems that were given in lectures, determine the number of vertices of degree 5.
4. Two trees with the same vertex set $\{1, 2, \ldots, n\}$ are **distinct** if their edge sets are not equal. Use mathematical induction to prove that for each integer $n \geq 2$, the number of distinct trees with vertex set $\{1, 2, \ldots, n\}$ is at least $(n-1)!$.

Solutions

1. A tree with 11 vertices has $e = 10$ edges, so by the Handshake Theorem, the sum of degrees is $2e = 20$. We are given that exactly four vertices have degree 1 and exactly one vertex has degree 4. Let $v_1, v_2, \ldots, v_6$ be the remaining vertices whose degrees are to be determined. We have

$$\sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20$$

$$\sum_{i=1}^{6} \deg(v_i) = 12.$$

None of these six vertices $v_1, v_2, \ldots, v_6$ can have degree 1 (since there are exactly four vertices of degree 1, already accounted for). Hence each has degree at least 2. Because six vertices of degree at least 2 have total degree 12, each must have degree exactly 2.

Thus the remaining six vertices all have **degree 2**.

2. T is a tree with p vertices and so must have $p-1$ edges. Now by the Handshake Theorem we know

$$2(p-1) = \sum_{i=1}^{p} \deg(v_i).$$

Using the known degrees we can write this as

$$\begin{aligned} 2(p-1) &= 6 \cdot 1 + 4 \cdot 3 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-1) &= 18 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2p - 2 - 18 &= \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-10) &= \sum_{i=1}^{p-10} \deg(v_i). \end{aligned}$$

Rewriting the final line as

$$\frac{\sum_{i=1}^{p-10} \deg(v_i)}{p-10} = 2, \qquad \text{i.e.} \qquad \frac{\deg(v_1) + \deg(v_2) + \cdots + \deg(v_{p-10})}{p-10} = 2,$$

we see that the average degree of the remaining $p-10$ vertices is 2. However, we know that there are no more vertices of degree 1. Thus each of the remaining $p-10$ vertices must have **degree exactly 2**.

3. Let x be the number of vertices of degree 5 and y the number of vertices of degree 1. Then, because the tree has 12 vertices, we have

$$x + y + 3 = 12.$$

This simplifies to give $x + y = 9$.

Now, since T is a tree on 12 vertices, it must have $e = 11$ edges. By the Handshake Theorem, the sum of degrees is $2e = 22$, so

$$3 \cdot 3 + 5x + 1 \cdot y = 22.$$

This simplifies to give $5x + y = 13$.

Subtracting $x + y = 9$ from $5x + y = 13$ gives $4x = 4$, hence $x = 1$. Therefore there is exactly **one** vertex of degree 5.

4. We prove by induction that the number of distinct trees with vertex set $\{1, 2, \dots, n\}$ is at least $(n-1)!$.

Basis: let $n = 2$. Here $(n-1)! = (2-1)! = 1$. There is exactly one tree on $\{1, 2\}$, namely the single edge $\{1, 2\}$. So the base case is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and there are at least $(k-1)!$ distinct trees on $\{1, 2, \dots, k\}$.

Now consider $n = k + 1$. We aim to show that there are at least $k!$ distinct trees on vertex set $\{1, 2, \dots, k, k+1\}$.

Let T be a tree on vertex set $\{1, 2, \dots, k\}$. For any choice of $m \in \{1, 2, \dots, k\}$, we form a graph T_m on vertex set $\{1, 2, \dots, k, k+1\}$ as follows: start with tree T, add a new vertex $k+1$, and the edge $\{k+1, m\}$.

Note that T_m is connected (since $k+1$ is joined to m, and T was connected). Also, T_m has no circuit because T is a tree and adding a new leaf does not create a circuit. Thus T_m is a tree. Moreover, different choices of m give rise to distinct trees T_m, because their edge sets are different.

By the inductive hypothesis, there are at least $(k-1)!$ choices for the tree T. Since there are k choices for the vertex m, there are at least $k \cdot (k-1)! = k!$ trees T_m on vertex set $\{1, 2, \dots, k+1\}$.

By the principle of mathematical induction, this completes the proof. $\square$

See also

- math1061[200] — assessment weights and the full lecture schedule
- Logic: logical-connectives[201] · logical-equivalence-laws[202] · conditional-statements[203] · valid-argument-forms[204] · determining-argument-validity[205] · quantified-statements[206]
- Number theory and proof: proof-techniques[207] · rational-and-irrational-numbers[208] · divisibility-and-factorisation[209] · modular-arithmetic[210] · gcd-lcm-and-euclidean-algorithm[211]
- Graph theory (§43–§46): [graphs] · walks-trails-and-circuits[212] · euler-circuits-and-trails[213] · adjacency-matrices[214] · incidence-matrices[215] · trees[216]

Proof Techniques — Direct, Counterexample, Contradiction, Contraposition

The four methods for establishing (or demolishing) a statement of the form $\forall x \in D, P(x) \to Q(x)$, plus the definitions every proof in this course is expected to unfold.

Definitions to prove from

Proofs are written by **demonstrating facts using the definitions** — so these have to be at your fingertips. Each is a biconditional: it can be used in either direction.

Term	Definition
n is **even**	$n = 2k$ for some integer k
n is **odd**	$n = 2k + 1$ for some integer k (equivalently $n = 2k - 1$ for some integer k)

[200] courses/math1061/math1061.pdf
[201] courses/math1061/logical-connectives.pdf
[202] courses/math1061/logical-equivalence-laws.pdf
[203] courses/math1061/conditional-statements.pdf
[204] courses/math1061/valid-argument-forms.pdf
[205] courses/math1061/determining-argument-validity.pdf
[206] courses/math1061/quantified-statements.pdf
[207] courses/math1061/proof-techniques.pdf
[208] courses/math1061/rational-and-irrational-numbers.pdf
[209] courses/math1061/divisibility-and-factorisation.pdf
[210] courses/math1061/modular-arithmetic.pdf
[211] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[212] courses/math1061/walks-trails-and-circuits.pdf
[213] courses/math1061/euler-circuits-and-trails.pdf
[214] courses/math1061/adjacency-matrices.pdf
[215] courses/math1061/incidence-matrices.pdf
[216] courses/math1061/trees.pdf

Term	Definition
n is **prime**	$n \in \mathbb{Z}$, $n > 1$, and $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then $(r = 1$ and $s = n)$ or $(r = n$ and $s = 1)$
n is **composite**	$n \in \mathbb{Z}$, $n > 1$, and $\exists r, s \in \mathbb{Z}^+$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$
r is **rational**	$\exists a, b \in \mathbb{Z}$ such that $r = \frac{a}{b}$ and $b \neq 0$
$d \mid n$	$d \neq 0$ and $n = dk$ for some integer k

Two facts used constantly, and worth naming explicitly when you lean on them:

- **Fact**: the sum, difference, and product of integers is an integer.
- **Fact**: every integer is either even or odd.

Parity

Almost every early proof in this course turns on whether something is even or odd, so the consequences of those two definitions are worth having ready rather than re-deriving:

	Result
even + even, odd + odd	even
even + odd	odd
even× anything	even
odd × odd	odd
consecutive integers	opposite parity — so two integers **two apart share their parity**

Each row follows from the two definitions by a one-line substitution. Subtraction behaves like addition throughout, since $m - n$ and $m + n$ differ by $2n$.

The "two apart" row is the whole content of the warm-up in 2026-07-27-welcome-and-intro-problems[217], where consecutive $p < q < r$ forces $p + r$ to be even and $r - p$ to be exactly 2, while pr is free to be either.

Prime vs. not-prime. For $n \in \mathbb{Z}^{>1}$, "n is not prime" means "n is composite". For $n \in \mathbb{Z}$ generally, "n is not prime" means "n is composite **or** $n \leq 1$" — the integers split into $\mathbb{Z}^{\leq 1}$, $\mathbb{Z}^{\text{prime}}$, and $\mathbb{Z}^{\text{composite}}$, and 1 and everything below it is in none of the latter two. This is why $n = 1$ is the standard counterexample to "every positive integer is prime or composite".

Warning: don't assume something that seems like an "obvious fact" until you have proven it, or can name the lecture or pre-work video it was proved in.

[217] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

The four methods

All four target $\forall x \in D, P(x) \to Q(x)$. Recall the truth table for $p \to q$ — the only row that makes it false is p true, q false:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Every method below is a different way of attacking that one row.

Direct proof (shows the statement is true)

> Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$. $\square$

Why suppose $P(x)$ is true, when $P(x) \to Q(x)$ holds anyway if $P(x)$ is false? Because the only case that could make the statement false is $P(x)$ true and $Q(x)$ false. Ruling that out is the whole job — the $P(x)$-false rows are true for free.

Disproof by counterexample (shows the statement is false)

> Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true. However, $Q(x)$ is false. So x is a counterexample and the statement is false.

A counterexample to $p \to q$ needs p **true** and q **false** — a value where the hypothesis fails proves nothing.

Proof by contradiction (shows the statement is true)

> Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true. That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false. ... Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$. This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. $\square$

The set-up comes straight from quantified-statements[218]: the negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D$ such that $P(x) \wedge \sim Q(x)$.

[218] courses/math1061/quantified-statements.pdf

Proofs of the statement $\forall x \in D,\ P(x) \to Q(x)$

Direct proof:

Let $x \in D$ and suppose $P(x)$.

...

Hence $Q(x)$. □

Shows the statement is true.

Disproof by counterexample:

Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true.

However, $Q(x)$ is false.

So x is a counterexample and the statement is false.

Shows the statement is false.

Proof by contradiction:

Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true.

That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false.

...

Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$.

This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. □

Shows the statement is true.

Proof by contraposition:

We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely that $\forall x \in D, \sim Q(x) \to \sim P(x)$.

Let $x \in D$ and suppose $\sim Q(x)$.

...

Hence, $\sim P(x)$. □

Figure 24: The skeletons of the four methods for a statement of the form x D, P(x) → Q(x). Three of the four establish the statement and one demolishes it, which is what the red verdict lines record.

Useful negations to have ready (see logical-equivalence-laws[219]):

$$\sim (p \vee q) \equiv \sim p \wedge \sim q \qquad \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \sim (p \to q) \equiv p \wedge \sim q$$

Proof by contraposition (shows the statement is true)

> We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely that $\forall x \in D, \sim Q(x) \to \sim P(x)$. Let $x \in D$ and suppose $\sim Q(x)$. ... Hence, $\sim P(x)$. $\square$

This is valid because $p \to q \equiv \sim q \to \sim p$ (see conditional-statements[220]).

Choosing a method

- **Contradiction is the most versatile**, but it needs more set-up, so a direct proof is often easier when one is available.
- **Contraposition** is the natural choice when $\sim Q(x)$ gives you something concrete to work with and $P(x)$ doesn't — typically when the conclusion is a negative statement ("r is irrational", "n is odd") whose negation is a definition you can expand.
- **Contradiction vs. contraposition**: a contraposition proof is a contradiction proof that never actually needs the assumption $P(x)$ — you derive $\sim P(x)$ from $\sim Q(x)$ alone. If your "contradiction" proof only ever uses the $\sim Q(x)$ half of the assumption, write it as a contraposition instead.
- **Counterexample vs. contradiction**: counterexample is a **disproof**, contradiction is a **proof**. They are not variants of each other.

Worked comparisons on the same statements live in the lecture notes: 2026-08-13-proof-by-contradiction[221] proves $\forall n \in \mathbb{Z}$, if n is odd then $3n+2$ is odd both directly and by contradiction, and 2026-08-13-proof-by-contraposition[222] works through statements where one method gets stuck and another doesn't.

Worked examples

Direct proof

$\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd.

[219] courses/math1061/logical-equivalence-laws.pdf
[220] courses/math1061/conditional-statements.pdf
[221] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[222] courses/math1061/2026-08-13-proof-by-contraposition.pdf

Let $n \in \mathbb{Z}$ and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Now

$$3n + 2 = 3(2k+1) + 2 = 6k + 5 = 2(3k+2) + 1.$$

Since $k \in \mathbb{Z}$, we have $3k + 2 \in \mathbb{Z}$, and hence $3n + 2$ is odd. □

For any integer x, if $x + 6 = 4y$ for some integer y, then $\frac{x}{2}$ is an odd integer.

Let $x \in \mathbb{Z}$ and suppose $x + 6 = 4y$ for some $y \in \mathbb{Z}$. Then $x = 4y - 6 = 2(2y - 3)$, so

$$\frac{x}{2} = \frac{2(2y-3)}{2} = 2y - 3 = 2(y-1) - 1.$$

Since $y \in \mathbb{Z}$ we have $2y - 3 \in \mathbb{Z}$, so $\frac{x}{2} \in \mathbb{Z}$; and $y - 1 \in \mathbb{Z}$, so by definition $\frac{x}{2}$ is odd. □

The sum of any pair of even integers is even.

Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence $m + n = 2k + 2\ell = 2(k + \ell)$, which is even. □

$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

Suppose $n \in \mathbb{Z}^+$ and $n \geq 4$. Factor $2n^2 - 5n + 2 = (2n-1)(n-2)$. Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers greater than 1. Hence the expression is composite. □

Disproof by counterexample

- **For all integers m and n, if $2m + n$ is odd then m and n are both odd.** Counterexample $m = 4, n = 5$: $2(4) + 5 = 13$ is odd, but m is even. (Not $m = 3, n = 5$ — there the conclusion holds; not $m = 3, n = 6$ or $m = 4, n = 6$ — there the hypothesis fails.)
- **$\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n+1$ is composite.** Take $n = 2$: both 2 and 3 are prime.
- **For each integer $n \geq 2$, the product of the first n primes minus 1 is prime.** Take $n = 4$: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, composite.
- **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** Take $x = 1, y = -2$: $4 > 1$ but $-2 \not> 1$.
- **$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** Take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1$. (See modular-arithmetic[223] for the floor function.)

[223] courses/math1061/modular-arithmetic.pdf

Disproof by proving the negation

When the statement to disprove is existential, a single counterexample isn't available — you must prove the universal negation.

$\exists n \in \mathbb{Z}^+$ **such that** $n^2 + 5n + 6$ **is prime.** This is false; the negation is $\forall n \in \mathbb{Z}^+$, $n^2 + 5n + 6$ is composite.

> Let $n \in \mathbb{Z}^+$. Now $n^2 + 5n + 6 = (n + 2)(n + 3)$. Since $n \geq 1$ we have $n + 2 > 1$ and $n + 3 > 1$, so $n^2 + 5n + 6$ is composite. □

(Because $n \geq 1$ forces $n^2 + 5n + 6 \geq 2$, "not prime" here does mean "composite".)

There is an even integer n **such that** $5n - 4$ **is prime.** False; prove $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

> Suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $5n - 4 = 10k - 4 = 2(5k - 2)$, which is even. The only even prime is 2; if $2(5k-2) = 2$ then $k = \frac{3}{5} \notin \mathbb{Z}$. Therefore $5n - 4$ is not prime. □

Proof by contradiction

$\forall m, n \in \mathbb{Z}$**, if** mn **is even, then** m **is even or** n **is even.**

> Suppose $\exists m, n \in \mathbb{Z}$ such that mn is even and both m and n are odd. Since m is odd, $m = 2k + 1$ for some $k \in \mathbb{Z}$; since n is odd, $n = 2\ell + 1$ for some $\ell \in \mathbb{Z}$ — **a new variable**, since m and n need not be equal. Now
>
> $$mn = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$
>
> Since $k, \ell \in \mathbb{Z}$, $2k\ell + k + \ell \in \mathbb{Z}$, so mn is odd. It is impossible for mn to be both even and odd, a contradiction. Therefore the original statement is true. □

$\forall n \in \mathbb{Z}$**, if** $3n^3 - 2$ **is odd, then** n **is odd.**

> Suppose the statement is false: $\exists n \in \mathbb{Z}$ such that $3n^3 - 2$ is odd and n is even. Since n is even, $n = 2a$ for some $a \in \mathbb{Z}$. Then
>
> $$3n^3 - 2 = 3(2a)^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$
>
> Since $a \in \mathbb{Z}$, $12a^3 - 1 \in \mathbb{Z}$, so $3n^3 - 2$ is even — a contradiction. Therefore the original statement is true. □

$\forall m, n \in \mathbb{Z}$**, if** $m + n$ **is even, then** m **and** n **are both even or both odd.**

Suppose the statement is false. Then $\exists m, n \in \mathbb{Z}$ such that $m+n$ is even but exactly one of m, n is even. **Without loss of generality**, assume m is even and n is odd — the other case (m odd, n even) follows because $m+n = n+m$. Thus $m = 2a$ for some $a \in \mathbb{Z}$ and $n = 2b+1$ for some $b \in \mathbb{Z}$. Now $m+n = 2a+2b+1 = 2(a+b)+1$, and $a+b \in \mathbb{Z}$, so $m+n$ is odd. This contradicts the assumption that $m+n$ is even. Therefore the original statement is true. □

For integers a and b, if $6a+3b$ is odd, then b is odd.

Suppose there exist integers a, b with $6a+3b$ odd and b even. Then $b = 2k$ for some $k \in \mathbb{Z}$, so $6a+3b = 6a+6k = 2(3a+3k)$, which is even — contradicting that $6a+3b$ is odd. □

For all positive integers x and y, $x^2 - y^2 \neq 1$.

Suppose $x, y \in \mathbb{Z}^+$ with $x^2 - y^2 = 1$. Factoring, $1 = (x-y)(x+y)$. Since x, y are positive integers we must have $x-y = 1$ and $x+y = 1$, so $2x = 2$ and $x = 1$; then $y = 0$, which is not a positive integer — a contradiction. □

Proof by contraposition

$\forall r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

We prove the contrapositive: $\forall r \in \mathbb{R}$, if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$. Suppose $r \in \mathbb{R}$ with $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Now $r^2 = \frac{a^2}{b^2}$. Since $a, b \in \mathbb{Z}$ we have $a^2, b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $r^2 \in \mathbb{Q}$. □

$\forall m, n \in \mathbb{Z}$, if mn is odd, then m and n are both odd.

We prove the contrapositive: $\forall m, n \in \mathbb{Z}$, if at least one of m, n is even then mn is even. Without loss of generality, assume m is even, so $m = 2k$ for some $k \in \mathbb{Z}$. Now $mn = (2k)n = 2(kn)$, and $kn \in \mathbb{Z}$, so mn is even. □

For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

Contrapositive: if a is even or b is even, then $(ab)^2$ is even. WLOG suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ and $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even. □

For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.

Contrapositive: if x is even or y is even, then $x^2(y^2-2y)$ is even. Here the two cases need separate treatment.

Case 1: x even. $x = 2k$ for some $k \in \mathbb{Z}$, so $x^2(y^2-2y) = 4k^2(y^2-2y) = 2(2k^2(y^2-2y))$, and $2k^2(y^2-2y) \in \mathbb{Z}$.

Case 2: y even. $y = 2\ell$ for some $\ell \in \mathbb{Z}$, so $x^2(y^2 - 2y) = x^2(4\ell^2 - 4\ell) = 2(x^2(2\ell^2 - 2\ell))$, and $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$.

In both cases $x^2(y^2 - 2y)$ is even. □

For any integer n, n^2 is odd if and only if n is odd. A biconditional needs both directions, and they want different methods:

($\Leftarrow$, direct) Suppose n is odd, so $n = 2k+1$. Then $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd.

($\Rightarrow$, contraposition) The contrapositive is: if n is even then n^2 is even. Suppose $n = 2k$. Then $n^2 = 4k^2 = 2(2k^2)$ is even. □

This lemma — **for all integers n, if n^2 is even then n is even** — is used in the proof that $\sqrt{2}$ is irrational (see rational-and-irrational-numbers[224]).

Common proof errors

The course explicitly tests spotting these. The seven below are the list given with the practice problems' §9 Q3 (see practice-problems[225], where the four proofs you are asked to find the errors in are worked):

- **Arguing from examples** — a single example never establishes a universal statement. ("$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = 1$. Proof: if $x = 10$ take $y = \frac{1}{10}$." Not a proof — and the statement is false, since $x = 0$ has no such y.)
- **Using the same variable to mean two different things** — "let $m = 2k + 1$ and $n = 2k$" only proves the case $m = n + 1$. Use a fresh variable for each quantity.
- **Jumping to the conclusion** — writing down the definition you need to satisfy and then asserting it holds, without exhibiting the witnesses.
- **Assuming what is to be proved** — starting from "$4a + 2b = 2\ell$" and manipulating both sides assumes the conclusion. Derive the conclusion; don't begin with it.
- **Confusion between what is known and what is to be shown.**
- **Use of the word *any* instead of *some*.**
- **Misuse of the word *if*.**

One more, not on that list: **forgetting to state your assumptions**, or forgetting to say where a variable lives ("for some $r, s \in \mathbb{Z}$"). Introduce every existential witness with its domain.

[224] courses/math1061/rational-and-irrational-numbers.pdf
[225] courses/math1061/practice-problems.pdf

See also

- quantified-statements[226] — the negations these proofs are built on
- conditional-statements[227] · logical-equivalence-laws[228]
- 2026-07-27-welcome-and-intro-problems[229] — the parity warm-up, the course's first proof-shaped problem
- proving-set-properties[230] — the element method, and these techniques applied to sets
- rational-and-irrational-numbers[231] · divisibility-and-factorisation[232]
- practice-problems[233] — §9 Direct Proofs and Counterexamples, with full worked solutions
- practice-problems[234] — §10 Proof by Contradiction, with full worked solutions
- practice-problems[235] — §11 Proof by Contraposition, with full worked solutions

Solving Recurrence Relations

recursive-definitions[236] builds a sequence out of its own earlier terms. This note goes the other way: given a recursive definition, find an **explicit formula** for the nth term, and prove the formula is right. See mathematical-induction[237] and strong-induction-and-the-well-ordering-principle[238] for the proof machinery the second method leans on.

Two ways of writing the same sequence

Every sequence here can be described twice over, and the two descriptions are worth naming precisely because the whole topic is moving between them:

	Shape	What it lets you do
Recurrence relation	$a_k = \dots a_{k-1} \dots$	get the next term from the ones before it
Explicit formula	$a_n = \dots n \dots$	get *any* term without computing the others

[226] courses/math1061/quantified-statements.pdf
[227] courses/math1061/conditional-statements.pdf
[228] courses/math1061/logical-equivalence-laws.pdf
[229] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[230] courses/math1061/proving-set-properties.pdf
[231] courses/math1061/rational-and-irrational-numbers.pdf
[232] courses/math1061/divisibility-and-factorisation.pdf
[233] courses/math1061/practice-problems.pdf
[234] courses/math1061/practice-problems.pdf
[235] courses/math1061/practice-problems.pdf
[236] courses/math1061/recursive-definitions.pdf
[237] courses/math1061/mathematical-induction.pdf
[238] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

The subscript is the tell. A rule written in k that mentions a_{k-1} is a recurrence relation; a rule written in n that mentions only n is an explicit formula.

Arithmetic and geometric sequences

The two standard families, in both forms — for a sequence $a_0, a_1, a_2, \ldots$:

	Recurrence relation	Explicit formula
Arithmetic	$a_k = a_{k-1} + d$ for integers $k \geq 1$	$a_n = a_0 + dn$ for integers $n \geq 0$
Geometric	$a_k = r \cdot a_{k-1}$ for integers $k \geq 1$	$a_n = a_0 \cdot r^n$ for integers $n \geq 0$

d is the **common difference** and r the **common ratio**. Both explicit formulas are the recurrence applied n times from a_0, which is why the index of the seed and the exponent agree: a_n is n steps away from a_0.

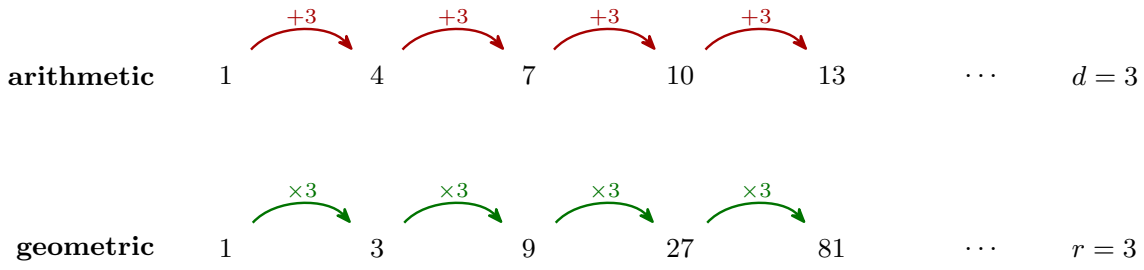


Figure 25: The two families as operations between consecutive terms. Arithmetic adds the same d at every step; geometric multiplies by the same r. Reading a sequence means testing the gaps: constant differences means arithmetic, constant ratios means geometric.

Worked the other way, from terms to a formula: $2, 6, 18, 54, \ldots$ multiplies by 3 each step, so $r = 3$; the seed is $a_0 = 2$; hence $a_n = 2 \cdot 3^n$.

Telling them apart

Deciding which family a run of terms belongs to is a matter of computing the gaps both ways, not of eyeballing.

Do $\frac{5}{8}, \frac{5}{2}, 10$ sit in an arithmetic sequence, a geometric one, both, or neither?

Put everything over the same denominator — $\frac{5}{8}, \frac{20}{8}, \frac{80}{8}$ — and both tests become easy:

Test	First gap	Second gap	Verdict
Differences	$\frac{20}{8} - \frac{5}{8} = \frac{15}{8}$	$\frac{80}{8} - \frac{20}{8} = \frac{60}{8}$	not equal — **not arithmetic**
Ratios	$\frac{5}{2} \div \frac{5}{8} = 4$	$10 \div \frac{5}{2} = 4$	equal — **geometric**, $r = 4$

So the answer is *geometric only*. The common trap is "both": a sequence that passes the ratio test has no obligation to pass the difference test, and here it plainly fails it.

Do $2, 2, 2$? This one is **both**. The differences are all 0, so it is arithmetic with $d = 0$; the ratios are all 1, so it is geometric with $r = 1$. It is **a constant sequence** $a_n = c$, which is what you get from $d = 0$ on one side and $r = 1$ on the other. The constant sequences are the *whole* of the overlap and not merely examples of it: $a_0 + dn$ and $a_0 r^n$ can agree for every n only if $d = 0$, and then both are constant.

> One convention worth knowing: many texts require $a_0 \neq 0$ and $r \neq 0$ for a geometric sequence, which excludes the all-zeros sequence $0, 0, 0, \ldots$ — every r satisfies $0 = r \cdot 0$, so the common ratio would not be determined. $2, 2, 2$ is unaffected.

From a recursive definition to an explicit formula

The workflow is always the same three steps:

1. **Calculate** the first few terms from the recursive definition.
2. **Guess** an explicit formula that fits them.
3. **Prove** the guess is correct.

Step 3 is not optional, and it is the whole difficulty: any finite run of terms is consistent with infinitely many formulas (see sequences-and-summations[239] on why listing terms never defines a sequence). Two methods are available.

	Method 1	Method 2
What you show	the formula gives the right initial conditions, *and* satisfies the recurrence relation	the formula holds for every n, by (strong) mathematical induction
In a word	quicker	rigorous

[239] courses/math1061/sequences-and-summations.pdf

Why Method 1 is a proof and not just a check

Method 1 can look like it is only testing a couple of cases, so it is worth seeing why it settles the matter. A recursive definition **determines its sequence uniquely**: the initial conditions fix the first terms, and the recurrence relation then forces every later one. So if your formula reproduces the initial conditions and obeys the same recurrence, it generates the same sequence term by term — there is nowhere for the two to diverge. That is the entire content of Method 1, and it is why the two checks it makes are exactly the two halves of the definition.

Method 2 makes that argument explicitly rather than appealing to it, which is why it is the more rigorous of the two and the one to use when a question says "prove by induction".

The Method 1 template

Given a guess $a_n = f(n)$:

- **Initial conditions.** Substitute the seed index into f and check it returns the stated value. One check per initial condition.
- **Recurrence relation.** Write down both sides separately, substituting the guess wherever an earlier term appears, and show they agree:

$$\text{LHS} = a_k = f(k) \qquad \text{RHS} = (\text{the recurrence, with } f(k-1),\ f(k-2),\ \ldots \text{ substituted})$$

Set the two sides out under the labels **LHS** and **RHS** and meet in the middle. That keeps you from the circularity of starting with what you are trying to prove.

The Method 2 template

Take $P(n)$ to be the predicate $a_n = f(n)$ and run an induction. Which induction depends on the recurrence:

The recurrence reaches back	Use	Basis step needs
one term (a_{k-1})	ordinary induction (MI)	one base case
two or more terms ($a_{k-1}, a_{k-2}, \ldots$)	strong induction (SMI)	one base case per initial condition

The rule is not arbitrary: to get $P(k+1)$ from a recurrence mentioning a_{k-1}, you need $P(k-1)$ as well as $P(k)$, and only the strong hypothesis hands you both.

Worked examples

A recurrence reaching back one term

$c_1 = 1$ and $c_k = c_{k-1} + 2^k$ for each integer $k \geq 2$. Is this the sequence $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$?

Method 1.

Initial condition ($n = 1$): $c_1 = 2^{1+1} - 3 = 4 - 3 = 1$

Recurrence relation:

$$\text{LHS} = c_k = 2^{k+1} - 3$$
$$\text{RHS} = c_{k-1} + 2^k = (2^{(k-1)+1} - 3) + 2^k = 2^k + 2^k - 3 = 2(2^k) - 3 = 2^{k+1} - 3$$

LHS = RHS, so the formula satisfies the recurrence. **The statement is true.**

Method 2. Let $P(n)$ be the predicate $c_n = 2^{n+1} - 3$.

Basis step. $c_1 = 1$ by the recursive definition, and $2^{1+1} - 3 = 4 - 3 = 1$, so $P(1)$ is true.

Inductive hypothesis. Suppose $P(k)$ is true for some integer $k \geq 1$, i.e. $c_k = 2^{k+1} - 3$. Then

$$c_{k+1} = c_k + 2^{k+1} = (2^{k+1} - 3) + 2^{k+1} = 2(2^{k+1}) - 3 = 2^{k+2} - 3$$

so $P(k+1)$ is true. Hence by mathematical induction $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$. ■

Note the shape of the inductive step: substitute the recurrence, then the hypothesis, then collect. The two 2^{k+1} terms combining into 2^{k+2} is the only real move.

A recurrence reaching back two terms

$b_0 = 0$, $b_1 = 1$ and $b_k = \frac{1}{2}(b_{k-1} + b_{k-2} + 1) + 3(k-1)$ for each integer $k \geq 2$.

Calculating terms. Each one uses the two before it:

$$b_2 = \tfrac{1}{2}(1 + 0 + 1) + 3(1) = 1 + 3 = 4$$
$$b_3 = \tfrac{1}{2}(4 + 1 + 1) + 3(2) = 3 + 6 = 9$$
$$b_4 = \tfrac{1}{2}(9 + 4 + 1) + 3(3) = 7 + 9 = 16$$

giving $0, 1, 4, 9, 16, \ldots$ — **guess $b_n = n^2$ for all integers $n \geq 0$.**

Method 1.

Initial conditions: $b_0 = 0^2 = 0$ and $b_1 = 1^2 = 1$ — two conditions, two checks.

Recurrence relation:

$$\text{LHS} = b_k = k^2$$

$$\begin{aligned}\text{RHS} &= \tfrac{1}{2}\big((k-1)^2 + (k-2)^2 + 1\big) + 3(k-1)\\ &= \tfrac{1}{2}\big(k^2 - 2k + 1 + k^2 - 4k + 4 + 1\big) + 3k - 3\\ &= \tfrac{1}{2}\big(2k^2 - 6k + 6\big) + 3k - 3\\ &= \big(k^2 - 3k + 3\big) + 3k - 3\\ &= k^2\end{aligned}$$

LHS = RHS, so the explicit formula satisfies the recurrence relation.

Method 2, by strong induction — two terms back, so SMI and two base cases.

Basis step. $b_0 = 0$ and $0^2 = 0$, so $P(0)$ holds; $b_1 = 1$ and $1^2 = 1$, so $P(1)$ holds.

Inductive hypothesis. Suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are each true. Then

$$\begin{aligned}b_{k+1} &= \tfrac{1}{2}\big(b_k + b_{k-1} + 1\big) + 3\big((k+1) - 1\big)\\ &= \tfrac{1}{2}\big(k^2 + (k-1)^2 + 1\big) + 3k\\ &= \tfrac{1}{2}\big(k^2 + k^2 - 2k + 1 + 1\big) + 3k\\ &= \tfrac{1}{2}\big(2k^2 - 2k + 2\big) + 3k\\ &= k^2 - k + 1 + 3k\\ &= k^2 + 2k + 1 = (k+1)^2\end{aligned}$$

so $P(k+1)$ is true, and by SMI $b_n = n^2$ for each integer $n \geq 0$. ■

The hypothesis is used **twice** here — once for b_k and once for b_{k-1} — which is precisely what ordinary induction could not have supplied.

The same sequence, a different recursive definition

Find a *different* recursive definition of $\{b_n\}_{n\geq 0}$.

Once the explicit formula is known this is easy, and it makes the point that **a sequence does not have one recursive definition**. Look for a one-term recurrence $b_n = b_{n-1} + p$ and solve for the step p:

$$n^2 = (n-1)^2 + p \implies p = n^2 - (n-1)^2 = 2n - 1$$

so $b_0 = 0$ and $b_n = b_{n-1} + (2n-1)$ for all integers $n \geq 1$ defines the same sequence — the familiar fact that the squares are the running totals of the odd numbers. Note it needs only **one** initial condition where the original needed two.

A recurrence that is not a polynomial

$d_0 = 1$ and $d_k = \dfrac{d_{k-1}}{1 + d_{k-1}}$ for each integer $k \geq 1$.

Calculating terms. The useful move is multiplying by a disguised 1 to clear the fraction inside the fraction:

$$d_1 = \frac{1}{1+1} = \frac{1}{2}$$

$$d_2 = \frac{\frac{1}{2}}{1+\frac{1}{2}} \cdot \frac{2}{2} = \frac{1}{2+1} = \frac{1}{3} \qquad d_3 = \frac{\frac{1}{3}}{1+\frac{1}{3}} \cdot \frac{3}{3} = \frac{1}{3+1} = \frac{1}{4}$$

giving $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ — **guess** $d_n = \dfrac{1}{n+1}$ **for all integers** $n \geq 0$**.**

That $\times \frac{k}{k}$ trick is worth keeping: multiplying numerator and denominator by the denominator of the inner fraction turns a compound fraction into a simple one in one step, with no common-denominator bookkeeping.

Method 1.

Initial condition ($d_0 = 1$): $d_0 = \dfrac{1}{0+1} = 1$

Recurrence relation:

$$\text{LHS} = d_k = \frac{1}{k+1} \qquad \text{RHS} = \frac{d_{k-1}}{1+d_{k-1}} = \frac{\frac{1}{k}}{1+\frac{1}{k}} \cdot \frac{k}{k} = \frac{1}{k+1}$$

LHS = RHS.

Method 2, by ordinary induction — the recurrence reaches back one term, so MI and one base case.

Basis step. $d_0 = 1$ from the definition and $\frac{1}{0+1} = 1$, so $P(0)$ is true.

Inductive hypothesis. Suppose $P(k)$ is true for some integer $k \geq 0$. Then

$$d_{k+1} = \frac{d_k}{1 + d_k} = \frac{1/(k+1)}{1 + 1/(k+1)} = \frac{1/(k+1)}{(k+2)/(k+1)} = \frac{1}{k+1} \cdot \frac{k+1}{k+2} = \frac{1}{k+2}$$

which is $\frac{1}{(k+1)+1}$, so $P(k+1)$ is true. By MI, $d_n = \dfrac{1}{n+1}$ for each integer $n \geq 0$. ■

The Tower of Hanoi

> Given a tower of 8 discs of decreasing size on one of three pegs, transfer the whole tower to another peg, subject to two rules: **move only one disc at a time**, and **never move a larger disc onto a smaller one**. Is there a solution, and if so what is the fewest number of moves?

This is the standard example of a recurrence that comes out of an argument rather than out of a formula. For $n \geq 1$ let m_n be the **minimum number of moves** needed to transfer a tower of n discs from one peg to another.

Small cases first: $m_1 = 1$ — move the single disc. $m_2 = 3$ — small disc to the spare peg, large disc to the target, small disc back on top.

The general case is the recursive insight:

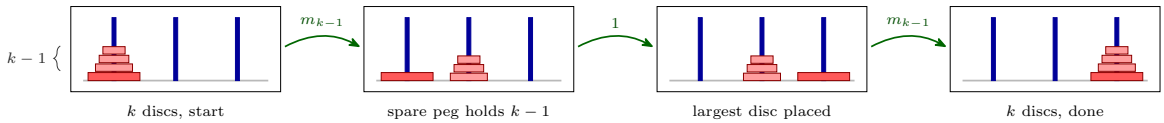


Figure 26: Why the recurrence doubles and adds one. Each box is one position of the three pegs, with discs as bars, the widest at the bottom, and the moves run left to right. To move k discs you must at some point move the largest, and it can only go onto an empty peg — so the other $k-1$ discs have to be parked on the spare peg first, then brought back on top afterwards. Two sub-transfers of $k-1$ discs, plus the single move of the largest. The $k-1$ smaller discs are drawn as a stack of three for legibility; nothing in the argument depends on how many there are.

Reading the picture off as arithmetic gives, for example, $m_4 = m_3 + 1 + m_3$, and in general

$$m_1 = 1 \qquad \text{and} \qquad m_k = 2m_{k-1} + 1 \text{ for all integers } k \geq 2$$

The explicit formula. The textbook (p. 310 in the 4th edition, p. 346 in the 5th) guesses $m_n = 2^n - 1$ for all integers $n \geq 1$. By Method 1:

Initial condition ($m_1 = 1$): $m_1 = 2^1 - 1 = 2 - 1 = 1$

Recurrence relation:

$$\text{LHS} = m_k = 2^k - 1$$
$$\text{RHS} = 2m_{k-1} + 1 = 2(2^{k-1} - 1) + 1 = 2 \cdot 2^{k-1} - 2 + 1 = 2^k - 1$$

LHS = RHS, so the guess is correct. The textbook proves the same result by mathematical induction — either method is acceptable.

So the eight-disc tower takes $2^8 - 1 = 255$ moves, and the answer to "is there a solution?" is yes, constructively, because the recursion *is* the algorithm.

See also

- recursive-definitions[240] — the other direction, and recursively defined sets
- sequences-and-summations[241] — sequence notation, and why initial terms never define a sequence
- mathematical-induction[242] · strong-induction-and-the-well-ordering-principle[243] — Method 2's machinery
- 2026-08-31-solving-recurrence-relations[244] — Lecture 16
- practice-problems[245] — §20 Solving Recurrence Relations, with full worked solutions

[240] courses/math1061/recursive-definitions.pdf
[241] courses/math1061/sequences-and-summations.pdf
[242] courses/math1061/mathematical-induction.pdf
[243] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[244] courses/math1061/2026-08-31-solving-recurrence-relations.pdf
[245] courses/math1061/practice-problems.pdf